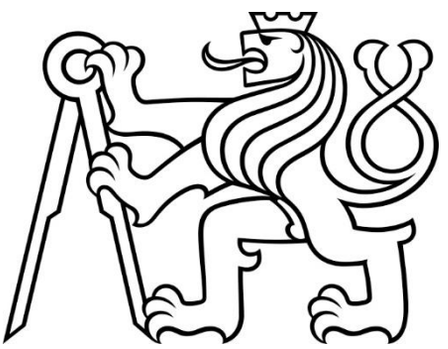
ČESKÉ VYSOKÉ
UČENÍ TECHNICKÉ
V PRAZE

FAKULTA
BIOMEDICÍNSKÉHO
INŽENÝRSTVÍ



# DIPLOMOVÁ PRÁCE

2019

JIŘÍ
FEIX

**ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE**

**Fakulta biomedicínského inženýrství**

**Katedra zdravotnických oborů a ochrany obyvatelstva**

# Analýza kybernetické kriminality v České republice

# Analysis of Cybercrime in the Czech Republic

Diplomová práce

Studijní program: Ochrana obyvatelstva
Studijní obor: Civilní nouzové plánování

Vedoucí práce: Ing. Josef Bernátek

**Bc. Jiří Feix**

**Kladno, květen 2019**

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

# ZADÁNÍ DIPLOMOVÉ PRÁCE

## I. OSOBNÍ A STUDIJNÍ ÚDAJE

| | | | | | |
|---|---|---|---|---|---|
| Příjmení: | **Feix** | Jméno: | **Jiří** | Osobní číslo: | **419312** |
| Fakulta: | **Fakulta biomedicínského inženýrství** | | | | |
| Garantující katedra: | **Katedra zdravotnických oborů a ochrany obyvatelstva** | | | | |
| Studijní program: | **Ochrana obyvatelstva** | | | | |
| Studijní obor: | **Civilní nouzové plánování** | | | | |

## II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

**Analýza kybernetické kriminality v České republice**

Název diplomové práce anglicky:

**Analysis of Cybercrime in the Czech Republic**

Pokyny pro vypracování:

Předmětem diplomové práce bude analýza postupů a dopadů registrované kybernetické kriminality na území České republiky. V teoretické části práce budou popsány jednotlivé druhy kybernetické kriminality, příslušná legislativa a rovněž budou uvedeny počty a závažnost registrované kybernetické kriminality na území České republiky. V praktické části práce bude provedeno pomocí analýzy a statistických metod vyhodnocení elementárních charakteristik časových řad, trendů a závažnosti registrované kybernetické kriminality na území České republiky. Dále budou vyhodnoceny dopady kybernetické kriminality na obyvatelstvo České republiky a pomocí statistických metod bude predikován předpokládaný trend této kriminality na další období. Zároveň budou vypracována konkrétní doporučení, jak se tomuto druhu kriminality bránit.

Seznam doporučené literatury:

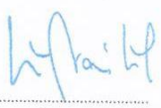
[1] POŽÁR, Josef, Základy teorie informační bezpečnosti, Praha: Vydavatelství PA ČR, 2007, ISBN 978-80-7251-250-8
[2] SMEJKAL, Vladimír, Kybernetická kriminalita, Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, ISBN 978-80-7380-501-2
[3] KOLOUCH, Jan, CyberCrime, Praha: CZ.NIC, z.s.p.o, 2016, ISBN 978-80-8816-815-7

Jméno a příjmení vedoucí(ho) diplomové práce:

**Ing. Josef Bernátek**

Jméno a příjmení konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **01.10.2018**
Platnost zadání diplomové práce: **18.09.2020**



prof. MUDr. Leoš Navrátil, CSc., MBA, dr.h.c.
podpis vedoucí(ho) katedry

prof. MUDr. Ivan Dylevský, DrSc.
podpis děkana(ky)

## Prohlášení

Prohlašuji, že jsem diplomovou práci s názvem Analýza kybernetické kriminality v České republice vypracoval samostatně pouze s použitím pramenů, které uvádím v seznamu bibliografických odkazů.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Kladně dne 16.05.2019

…….
podpis

## Poděkování

Na tomto místě bych rád poděkoval Ing. Josefu Bernátkovi za vedení, cenné rady a podporu při tvorbě diplomové práce. Poděkování patří i všem ostatním, kteří mi při zpracovávání práce pomáhali a také mě podporovali.

## Abstrakt

Tato diplomová práce se v teoretické části věnuje historii a současnému stavu kybernetické kriminality, zejména nejčastěji používaným metodám a jednotlivým druhům trestné činnosti. V praktické části této práce jsou analyzovány statistiky registrované trestné činnosti v rámci kybernetické kriminality za období 2011 – 2018 na území ČR. Tato data byla získána od Policie ČR.

Analýza byla zaměřena na základní popisné statistiky a elementární charakteristiky časových řad. Dále byla pomocí trendových funkcí vypočítána prognóza vývoje kybernetické kriminality na období následujících 3 let. Z výše popsaných statistik byly vyhodnoceny dopady na obyvatelstvo ČR a vypracováno několik doporučení na obranu proti kybernetické kriminalitě.

## Klíčová slova

Kybernetická kriminalita, analýza, Česká republika, kybernetický prostor, trestná činnost

## Abstract

This thesis in its theoretical part deals with history and present day cybercrime, particularly with most common methods and individual types of criminal activity. In its practical part provides analysis of registered criminal activity statistics of cybercrime from 2011 to 2018 in the Czech Republic. These statistical data were obtained from Police of the Czech Republic.

The analysis focused on basic descriptive statistics and fundamental characteristics of time series. Next the prognosis of cybercrime development for next three years was done by using trend function. The effects on Czech Republic population were concluded from the above mentioned statistics and suggestions for cybercrime defense were made.

## Keywords

Cybercrime, Analysis, Czech Republic, Cyberspace, Criminal Activity

# Obsah

# 1 ÚVOD

Trestná činnost v rámci kybernetického prostředí zažívá momentálně období velikého růstu. Bezpečnostní složky nestačí reagovat na expanzi kybernetické kriminality a zlepšování schopností pachatelů této trestné činnosti na celém světě. Tento trend se nevyhýbá ani České republice, kde úroveň kybernetické kriminality roste stejně rychle jako kdekoliv jinde ve světě.

Tato diplomová práce má za cíl komplexně zpracovat problematiku kybernetické kriminality a provést statistickou analýzu dat evidované trestné činnosti Policií České republiky.

V teoretické části se tato práce bude věnovat historii vývoje kybernetické kriminality ve světovém měřítku, jednotlivým druhům kybernetické kriminality a pojmům či technickým znalostem nutným k pochopení podstaty tohoto druhu trestné činnosti. V teoretické části se budeme také okrajově věnovat bezpečnostním složkám, které se kybernetickou kriminalitou zabývají.

V praktické části této práce bude provedena analýza registrované kybernetické kriminality na území České republiky, kdy budou pomocí grafů a tabulek popsány základní popisné statistiky a elementární charakteristiky časových řad. Dále bude v práci vypracována prognóza vývoje kybernetické kriminality na období následujících tří let pomocí vybraných trendových funkcí. Po prognóze na další období budou v práci rozebrány možné dopady kybernetické kriminality na obyvatelstvo a souhrn doporučení, jak se proti kybernetické kriminalitě efektivně bránit.

# 2 SOUČASNÝ STAV

## 2.1 Kybernetická kriminalita a související pojmy

### 2.1.1 Počátky kybernetické kriminality

S rozšiřováním výpočetních technologií pro širší okruh společnosti se paralelně rozšiřovalo riziko jejich kriminálního zneužití. Historicky můžeme říct, že co se výpočetních technologií a kybernetického prostoru týče, jsou bezpečnostní složky a justice celosvětově vždy o tři kroky pozadu než jejich protivníci, zejména kvůli široké škále možností výpočetních technologií a rovněž i kreativitě pachatelů ve vynalézání nových prostředků, jak obejít bezpečnostní opatření. V průběhu let se tak musely bezpečnostní složky učit, jak odhalovat, vyšetřovat a bránit společnost před tímto novým a velmi rychle se rozvíjejícím odvětvím kriminální činnosti. Ovšem kvůli nízké flexibilitě a rychlosti jakéhokoliv státního aparátu, byla reakční doba vždy velice pomalá.

Za první „virus“ se považuje program Creeper, který byl vytvořen inženýrem technologické společnosti BBN Robertem Thomasem přibližně v roce 1970. Společnost BBN hrála důležitou roli ve vývoji paketových sítí jako Arpanet a Internet. Robert Thomas v ní pracoval na vývoji operačního systému TENEX a právě na tomto systému se Creeper vyskytoval. Poté co se nahrál do systému, začal tisknout uživatelům soubory, následně našel jiný TENEX systém, otevřel si připojení, replikoval se v novém systému, ve starém se smazal a zanechal vzkaz „Catch me if you can“. Nutno podotknout, že se jednalo o samostatně replikující se program a nikoliv o virus, a to z toho důvodu, že byl vyvinut čistě pro experimentální účely, nikoliv aby způsobil jakoukoli škodu. V návaznosti byl vytvořen první antivirus zvaný Reaper, který v síti vyhledával kopie Creepera, aby je ničil. [1]

Na začátku sedmdesátých let se objevila technika „Phreaking“. Jednalo se o nabourání do telefonního systému pomocí zvukového tónu a zajištění si tak bezplatného užívání meziměstských hovorů. Za objevem této techniky stojí Joe Engressia, slepý chlapec obdařený absolutním sluchem, který zpozoroval, že při pískání u telefonického rozhovoru ho systém odpojí. Poté, co číslo vytočil znova a zapískal ve stejném tónu, byl opět odpojen. Telefonní společnost AT&T mu sdělila, že systém na přepínání hovorů funguje při tónu o frekvenci 2600 Hz, které se mu muselo podařit dosáhnout. Nedlouho po rozšíření této informace objevil John Draper, že píšťalka přibalená v cereáliích Cap'n Crunch vydává přesně 2600 Hz a umožňuje telefonování zdarma. Jedná se tak o první narušení systému, které způsobovalo větší škodu. [2]

Prvním odsouzeným člověkem za kybernetickou kriminalitu byl v roce 1981 Ian Murphy, přezdívaný také Captain Zap, který se provinil nabouráním do systému telefonické společnosti AT&T, kde změnil vnitřní hodiny tak, aby lidé dostali slevu za noční hovor během poledne. Byl odsouzen k 2500 hodinám veřejně prospěšných prací a 2,5 roku probace. [3]

V roce 1986 americký astronom Clifford Stoll, který byl v tu dobu zaměstnán jako administrátor sítě v národní laboratoři Lawrence Berkeley, vytvořil první digitální forenzní taktiku zvanou „Honeypot“, která spočívá v „lákání“ hackera do systému až do doby, dokud o něm administrátor nezíská dostatečná data potřebná k jeho identifikaci. Tento objev vedl k nalezení a zatčení Markuse Hesse a jeho dalších spolupracovníků, kteří kradli důležitá data z národní laboratoře v Lawrence Berkeley a dále je prodávali Ruské zpravodajské službě KGB. [3]

Brzy po objevení průniku do Berkeley se objevil Morris virus, pojmenovaný po svém tvůrci, studentovi Robertu Morissovi, který dokázal infikovat více než 6000 počítačů, které následně zpomaloval až na hranici použitelnosti a způsobit tak škody za 98 mil. dolarů. Po tomto a dalších incidentech byl americkým kongresem

přijat první zákon o kybernetické kriminalitě, který umožňoval pachatele takových činů potrestat vysokými tresty odnětí svobody. Díky tomu započala mnohá vyšetřování těchto aktivit a v roce 1990 tak vyvrcholila dvouletá operace FBI Sundevil. Pracovalo na ní 150 agentů, a FBI zadržela 42 počítačů a zajistila téměř 20 000 disket, které byly využity pro nelegální používání telefonních linek a kreditních karet. V následujících letech začal pravý rozmach kybernetické kriminality a také vzniklo mnoho národních i nadnárodních organizací, které tyto druhy zločinů vyšetřuje nebo brání občanská práva ostatních občanů při jejím vyšetřování, jako například Electronic Frontier Foundation. [3]

### 2.1.2 Definování kybernetické kriminality

V obecné rovině můžeme kybernetickou kriminalitu chápat jako trestnou činnost přímo spojenou s informačními technologiemi, ať už jako nástroj nebo cíl této trestné činnosti. Často užívaný název počítačová kriminalita nabízí variantu, že takový čin musí být spáchán v souvislosti s osobním počítačem (PC). Jak je ale již výše zmíněno, k páchání kybernetické kriminality může být využita jakákoliv informační technologie. Tato strohá definice ovšem není dostatečná, neb by zahrnovala i takové trestné činy jako napadení druhé osoby, při kterém by byl použit jako zbraň notebook, nebo by to v opačném případě mohla být krádež toho notebooku. Kolouch pak v komparaci několika dalších definic definuje kybernetickou kriminalitu ve třech kategoriích:

- *Trestné činy, jejichž individuálním objektem charakterizujícím skutkovou podstatu je přímo ochrana počítačového systému, jeho vybavení a součástí před specifickými druhy útoku resp. oprávněné zájmy osob nerušené užívání těchto technických prostředků.*
- *Trestné činy, kde je způsob spáchání prostřednictvím informační a komunikační techniky jedním ze znaků skutkové podstaty.*

- *Ostatní v úvahu připadající trestné činy, které nespadají do první ani druhé kategorie, avšak které mohou být v konkrétním případě též spáchány prostřednictvím informačních technologií a které odpovídají výše uvedené definici, neboť v rámci jejich odhalování a objasňování se mohou uplatnit obdobné postupy jako při vyšetřování trestných činů z 1. a 2. kategorie (např. obdobně zaměřené znalecké posudky).* [9]

Nyní si uvedeme několik klasifikací kybernetické kriminality podle různých organizací, dokumentů či autorů.

Úmluva Rady Evropy o kyberkriminalitě a její dodatkový protokol o xenofobii a rasismu dělí kybernetické trestné činy na:

- Trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů.
- Trestné činy související s počítači.
- Trestné činy související s obsahem.
- Trestné činy související s porušováním autorských práv a práv souvisejících.
- Šíření rasistických a xenofobních materiálů pomocí počítačových systémů.
- Rasisticky a xenofobně motivované vyhrožování.
- Rasově a xenofobně motivované útoky.
- Popírání schvalování nebo ospravedlňování genocidy nebo zločinů proti lidskosti. [15]

Dle Komise expertů na kybernetickou kriminalitu z roku 2000 lze kybernetické trestné činy rozdělit na:

- Dle pozice počítače při páchání trestné činnosti.
    - Cíl útoku.
    - Prostředek útoku.
- Podle typu činu.

    - Protiprávní jednání tradiční.
    - Protiprávní jednání nová. [9]

Akční plán evropské iniciativy eEroupe+ dělí kybernetickou trestnou činnost na:

- Zločiny porušující soukromí.
    - Nelegální sběr, uchovávání, modifikace, zveřejňování a šíření osobních dat.
- Zločiny se vztahem k obsahu počítače.
    - Dětská pornografie, rasismus, vyzývání k násilí apod.
- Ekonomické.
    - Neautorizovaný přístup, sabotáž, hackerství, šíření virů, počítačová špionáž, počítačové padělání a podvody.
- Zločiny se vztahem k duševnímu vlastnictví.
    - Autorské právo apod. [16]

Klasifikace počítačové trestné činnosti dle kriminologie.

- Neoprávněné zásahy do vstupních dat.
    - Změna vstupního dokladu pro zpracování počítačem.
    - Vytvoření dokladu obsahující nepravdivé údaje pro následné zpracování dat počítačem.
- Neoprávněné změny v uložených datech.
    - Manipulace s daty, neoprávněný zásah do nich a následný návrat k normálu.
- Neoprávněné pokyny k počítačovým operacím.
    - Přímý pokyn k provedení operace, či instalace softwaru provádějícího operace automaticky.
- Neoprávněné pronikání do počítačů, počítačového systému a jeho databází.

- Informativní vstup do databáze, bez využití informací.
- Neoprávněné užívání informací pro vlastní potřeby.
- Změny, ničení či nahrazování informací jinými.
- Nelegální odposlech a záznam provozu elektronické komunikace.

- Napadení cizího počítače, programového vybavení a souborů dat v databázích.
  - Vytváření programů sloužících k napadení.
  - Zavedení viru do programového počítače.
  - Vlastní napadení viry, či jinými programy. [9]

### 2.1.3 Pojmy související s kybernetickou kriminalitou

**Kyberprostor**

Slovo kyberprostor (Cyberspace) jako první použil americký spisovatel Wiliam Gibson ve své cyberpunkovém románu Neuromancer z roku 1984 a definoval ho jako: *„Konsenzuální halucinace prožívaná denně miliardami legitimních operátorů, v každém národě, dětmi, které se učí matematickým pojmům... grafické zobrazení dat abstrahovaných z pamětí každého počítače v lidské společnosti. Nepředstavitelná komplexita. Linie světla rozprostírající se v neprostoru mysli, klastry a konstelace dat. Jako světla velkoměsta, vzdalující se..."*[4] Toto literární, vizionářské a metaforické pojetí kybernetického prostoru se stalo vzorem následujících let, i když sám Gibson později termín kyberprostoru kritizoval, tak se díky úspěchu jeho díla napevno spojil se světem internetu a informačních technologií.

V dalších letech se objevovali nové definice jako například Deklarace Nezávislosti Kyberprostoru od zakladatele EFF J.P. Barlowova nebo Hakenovo

pojetí kybernetického prostoru. [5] V dnešní době neexistuje žádná plošně uznávaná definice kybernetického prostoru na vědecké úrovni. Například F. D. Kramer ve své publikaci Cyberpower and National Security udává, že existuje 28 různých definic výrazu kybernetický prostor. [6] Světové vlády a organizace si definici většinou upravují podle vlastních legislativních potřeb. Mezinárodní organizace pro standardizaci (ISO) definuje kybernetický prostor jako *„Komplexní prostředí vyplývající z interakcí lidí, softwaru a služeb na internetu prostřednictvím technologických zařízení a sítí k němu připojených, přičemž neexistuje v žádné fyzické formě.“ [7]* Tato definice podle mne jasně a srozumitelně vystihuje podstatu dnešního kybernetického prostoru v jeho surové podobě.

Jako materiální podstatu vzniku kyberprostoru považujeme internet, který poskytuje ono nutné spojení mezi zařízeními a vytváří tak síť. Počátky internetu lze datovat do roku 1836, kdy vznikla první telegrafní síť, která přenášela zprávy v Morseově abecedě složené z čárek a teček, což je podobné způsobu, jak mezi sebou komunikují počítače pomocí binárního kódu, tedy jedniček a nul. Internet jak ho známe dnes, se začal rodit během studené války, kdy v padesátých letech začala americká ARPA (Advanced Researsch Project Agency) a později DARPA (Defence Advanced Researsch Project Agency) pracovat způsobu komunikace, která by nebyla omezena nukleárním útokem. V roce 1967 byl spuštěn projekt ARPANET, který spojoval počítače v univerzitních kampusech napříč USA a s postupným rozšiřováním za pomoci NSF (National Science Foundation) rozrostl do internetu. [8]

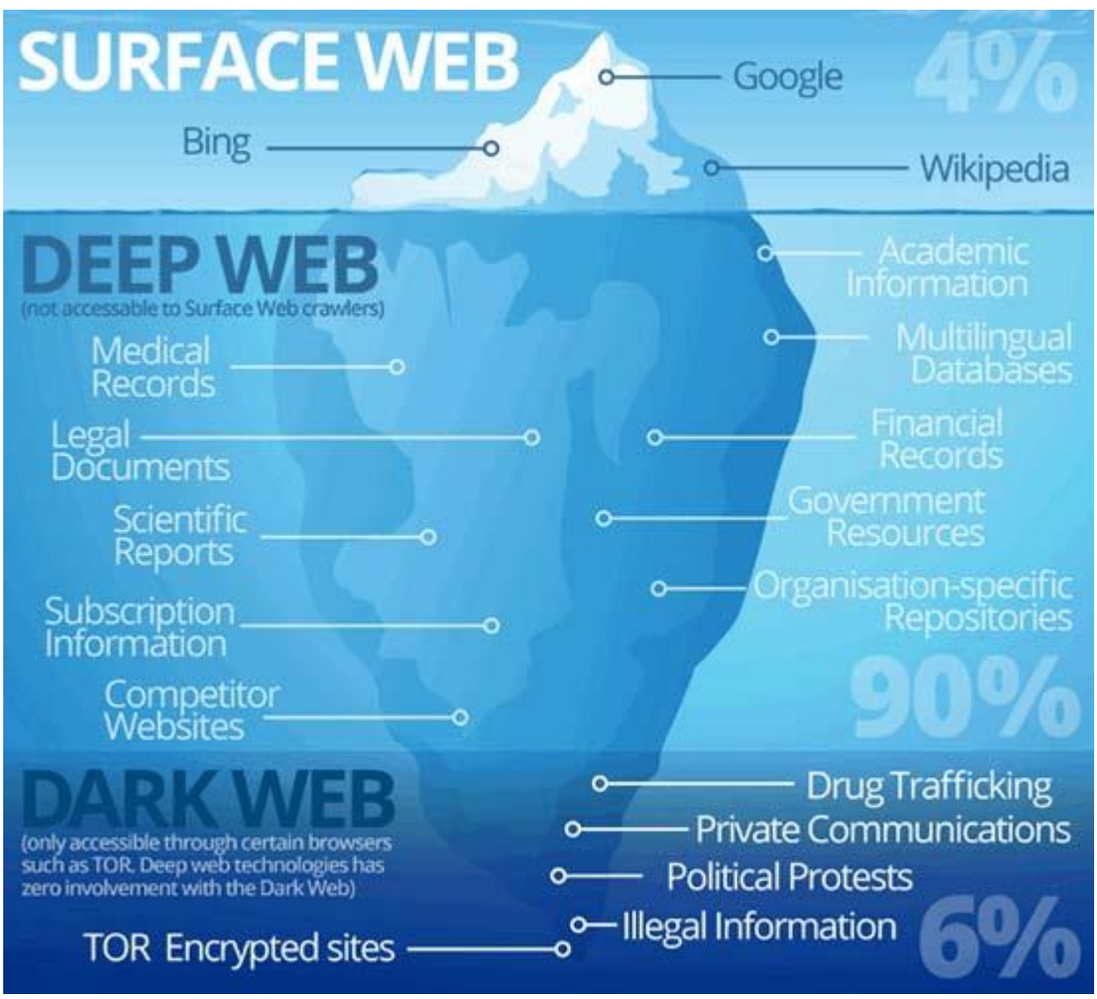
Technologicky je internet složen z celosvětové distribuované počítačové sítě, která je složena z jednotlivých menších sítí, navzájem propojených pomocí protokolů IP. Vzájemná komunikace a přenos dat jsou zajištěny fyzicky přítomnou materiální sítí, která vede signál vzduchem, kabely nebo jinými přenosovými médii. Vzniká tak kybernetický prostor, který je přímo vázaný na hardware, jenž jej tvoří. Díky neustále rozšiřující se síti je kyberprostor víceméně neomezený, avšak

jako nehmotné médium, schopné se aktivně adaptovat na poškození svého materiálního média. Paradoxně ovšem při absolutním kolapsu celé hmotné sítě dojde k nevratnému poškození, či dokonce zániku celého kyberprostoru. [9]

Kybernetický prostor využívá 55 % veškeré světové populace. K 30. lednu 2018 to bylo více než 4,2 mld. lidí. Nejvíce uživatelů na počet obyvatel je v Asii a to zhruba 2 mld., což představuje 49 % celkové populace. Na evropském kontinentu je k internetu připojeno 85 % populace a v Severní Americe dokonce 95 % veškerého obyvatelstva. Nejméně je rozšířen internet v Africe, kde má možnost připojení 36 % obyvatel. Přestože byly první základy internetu položeny před více než čtyřiceti lety, jeho největší rozšíření se událo v posledních dvaceti letech. [10]

Kybernetický prostor můžeme rozdělit na tři části. První je takzvaný „Surface Web" neboli viditelný web. Jedná se o část internetu, která je jednoduše přístupná pomocí standardních vyhledávačů jako je Google, Facebook, Wikipedia a v České republice velice oblíbený Seznam.cz. Tato část internetu je všem přístupná a vyskytuje se na ní pouhá 4 % veškerého obsahu na internetu. Druhou a největší částí, na které se nachází až 90 % všech dat je „Deep Web". Jedná se poloprivátní nebo privátní sítě, které jsou využívány v rámci společností a organizací. Taková síť se označuje jako Intranet. Intranet se používá k přenosu dat a informací v rámci nebo mezi danými subjekty. Důležitým znakem těchto sítí je, že nejsou přístupné pomocí standardního internetového vyhledávače. Poslední částí je Dark Web neboli Dark Net. Tato část internetu je přístupná za využití specifických softwarových nástrojů, mezi které lze zařadit prohlížeč TOR. Návody jak se na Dark Web dostat, jsou běžně k nalezení na Surface Webu a můžeme tak říct, že je s určitou mírou zručnosti dostupný všem uživatelům. Připojení na Dark Webu probíhá většinou na principu P2P sítí a jeho adresy se mohou skládat, jako kupříkladu v síti TOR, z písmen a číslic s koncovkou .onion. Dark Web je veřejností hodnocen spíše negativně. I přes značně sugestivní název má však i své světlé stránky. Například lidé v zemích, kde je omezena svoboda slova a probíhá cenzura,

se tak mohou svobodně vyjadřovat a získávat neomezený přístup k informacím. Na druhou stranu Dark Web funguje i jako trh s nelegálním zbožím, uživatel si zde může pořídit čísla kreditních karet, ukradené účty na platformy jako je Netflix, lidské orgány, drogy, zbraně, falešné doklady a diplomy apod. Jako měna se při transakcích používají hlavně kryptoměny, mezi nejoblíbenější patří BitCoin. Jedním z nejznámějších tržišť na Darknetu byl takzvaný Silk Road, založený v roce 2011 Rossem Ulbrichtem a uzavřený FBI v roce 2013. Silk Road byl postaven na principu dvojí anonymity s utajenou totožností prodejce i nakupujícího. Podle různých zdrojů se uvádí, že obrat Silk Roadu byl za dobu jeho působení 9 519 664 Bitcoinů, což při kurzu 3825 amerických dolarů za jeden BitCoin k 26.2.2019 činí 36, mld. amerických dolarů a bylo zde registrováno 957 079 uživatelů. [9,12]




*Obrázek 1 Rozdělení kyberprostoru. [11]*

**Kybernetický útok**

Dle výkladového slovníku kybernetické bezpečnosti můžeme definovat kybernetický útok jako *„Útok na IT infrastrukturu, za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.“* [13]

Tato definice je ale nedostatečná. Nezahrnuje veškeré negativní aktivity, které se v kybernetickém prostoru odehrávají. Kolouch definuje kybernetický útok jako *„Jakékoli protiprávní jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby. Tato jednání nemusí mít vždy podobu trestného činu, podstatné je, že narušují běžný způsob života poškozeného. Kybernetický útok může být dokonán, stejně jako může být ve stádiu pokusu.“* [9] Dále se zmiňuje o tom, že ne každý kybernetický útok musí být trestným činem, ovšem kybernetický trestný čin musí být kybernetickým útokem. Je tomu tak především kvůli absenci trestněprávní normy, kvůli čemuž se takové jednání nejčastěji řeší ve správněpravní či občanskoprávní rovině, nebo se může jednat o čin, který není postižitelný žádnou právní normou. [9]

Zákon o kybernetické bezpečnosti v § 7 definuje pojmy, které lze přirovnat ke kybernetickému útoku, a to kybernetickou bezpečnostní událost a kybernetický bezpečnostní incident, kdy *„kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací“* Kybernetický bezpečnostní incident je definován jako *„narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity komunikací v důsledku kybernetické bezpečnostní události.“* [14]

**Počítačový systém**

Počítačový systém je pojem, který je primárně používán v souvislosti s legislativou, a to s trestním zákoníkem. Tento pojem byl do legislativy ČR včleněn po podpisu Úmluvy o kyberkriminalitě. Tato úmluva ho definuje jako *„jakékoli zařízení nebo skupina propojených nebo přidružených zařízení, z nichž jedno nebo více provádí automatické zpracování dat podle programu.“ [15]*

Více užívaný pojem počítač má také více definic. Podle výkladového slovníku výpočetní techniky je tedy pojem počítač definován jako *„souhrnné označení pro zařízení vyznačující se následujícími rysy: zařízení obsahuje centrální procesorovou jednotku, schopnou řídit se programovým kódem a schopnou ovládat přidružené periferie a další části počítače; dále zařízení obsahuje prvek pro vstup dat (klávesnice, myš), médium pro ukládání dat (paměť, disk, disketa) a zobrazovací zařízení“*. [17] Tato definice je i přes své stáří stále přesná, stačí pouze rozšířit o tvrzení, že vstup dat neboli ovládání, které není primárně omezeno klávesnicí a myší, a že počítač taktéž nemusí nutně obsahovat zobrazovací zařízení.

Počítač se ale skládá ze dvou hlavních částí. Jsou jimi hardware a software. Hardware je část počítače, která je hmotná. Při bližším rozdělení na vnitřní a periferní hardware je vnitřní hardware technologická součást počítačového systému jako procesor, paměť RAM, diskové úložiště nebo třeba základní deska. Mezi periferní hardware řadíme veškerá zařízení, které je připojeno k počítači externě a není jeho pevnou součástí například v počítačové skříni. Jedná se tedy třeba o klávesnici, myš, monitor nebo třeba i externí disk. Oproti tomu software je součást počítače, která je nehmotná. Jedná se o operační systém, aplikace, které jsou naprogramovány tak, aby prováděli specifické operace pomocí hardwaru. Můžeme tedy říci, že tyto dvě součásti jsou od sebe neoddělitelné. Hardware nemůže samostatně plně fungovat bez softwaru a naopak.

**Data a informace**

Úmluva o kyberkriminalitě počítačová data specifikuje jako *„jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem.“*. [15]

Požár ve své knize definuje data jako *„fakta, čísla, události, grafy, mapy, transakce atd., které byly zaznamenán. Jsou základním materiálem, surovinou pro informace.“*. [18] Data jsou tedy prvky s informační hodnotou, které následně zpracovává počítač. Ty jsou tak uchovávány v ucelených souborech různého typu a jsou zpracovávány, aby následně utvořily informaci. [9]

Z hlediska trestního práva jsou data uchovávána na nosičích informací. Nosičem informací se v rámci trestního zákoníku rozumí jakékoli paměťové médium, které uchovává data v digitální podobě. [9]

Informacemi rozumíme *„údaje, které byly zpracovány do podoby užitečné pro příjemce. Každá informace je tedy údajem, datem, ale jakákoli uložená data nemusejí být nutně informací. [18]* Informace považujeme za nadstavbu dat, kdy jsou data vnímána v nějakém kontextu jako fakt a nesou nějaký význam, který je pochopitelný pro člověka. [9]

**Počítačové sítě**

Počítačovou sítí rozumíme *„soubor počítačů spolu s komunikační infrastrukturou (komunikační linky, technické vybavení, programové vybavení a konfigurační údaje), jejímž prostřednictvím si (počítače) mohou vzájemně posílat a sdílet data.“* [13]

Počítačové sítě můžeme rozdělit do několika kategorií. Pro potřeby této práce je rozdělíme do třech hlavních skupin.

1) **Rozdělení podle rozsahu.**
    a) **PAN (Personal Area Network – Osobní síť).** Jedná se o osobní síť, kterou využívá pro své potřeby zpravidla jednotlivec nebo domácnost. Skrze tuto síť se propojují jednotlivé počítačové systémy většinou typu osobních počítačů nebo telefonů za pomoci technologií WiFi nebo Bluetooth. Specifikum PAN sítě je, že přenos probíhá na malé vzdálenosti a mezi danými systémy se nepřenáší velké objemy dat. Zařízení, která jsou připojena v takové síti, se připojují např. do tzv. Internetu věcí (IoT)
    b) **LAN (Local Area Network – Lokální síť).** Označení LAN se používá pro místní sítě, ve kterých dochází k propojení jednotlivých uzlů v rámci jedné nebo i více budov. Propojení uzlů může být provedeno pevnou (kabelovou) formou nebo za pomocí bezdrátové sítě. Sítě LAN mají vyšší přenosovou rychlost a přenáší tak větší objemy dat než sítě PAN. Síť LAN tak bývá využívána v rámci celých organizací, ale může být vybudována i v rámci domácnosti pro komunikaci mezi počítačovými systémy, tiskárnami apod.
    c) **MAN (Metropolitan Area Network – Metropolitní síť).** Sítě MAN propojují navzájem několik sítí LAN v rámci městské zástavby na vzdálenosti jednotek až desítek kilometrů. Někdy bývá také označována jako síť WAN
    d) **WAN (Wide Area Network – Vzdálená počítačová síť).** Sítě WAN propojují vzdálené LAN nebo MAN sítě. Geograficky se jedná o propojení sítí v rámci států, kontinentů nebo i celého světa.
2) **Rozdělení podle postavení síťových uzlů.**
    a) **Peer-to-peer (P2P – klient-klient)** je sítí, kdy dochází k přímé komunikaci mezi jednotlivými uživateli (klienty). Jedná se o síť, která se nedá nijak centrálně spravovat a používá se primárně ke sdílení souborů. Nejčastěji bývá využívána k šíření a stahování filmů, her nebo programů, které jsou zbaveny ochranných mechanismů autorů a porušují tak autorské právo.

b) **Klient-server** je druhem sítě kdy je server nadřazen počítačovým systémům uživatelům (klientům), kteří žádají o přístup do takové sítě. Nejčastěji se jedná o služby jako je e-mail nebo datová uložiště.

3) **Rozdělení podle vlastnictví sítí.**

a) **Privátní síť** je počítačovou sítí, která využívá privátní IP adresy, takové adresy jsou používány v rámci sítě LAN. Jestliže privátní síť potřebuje připojení k internetu, musí požívat překlad síťových adres (NAT), nebo proxy server.

b) **Veřejná síť** je počítačovou sítí, do které se může připojit kdokoli, kdo přistoupí na podmínky provozovatele, respektive za její užívání zaplatí. Uživatel se přes tuto síť může připojovat k jiné síti nebo k internetu. Vzhledem k tomu, že takové sítě většinou nemají žádné omezení, bývá často bezpečnostním rizikem pro uživatele, který se k takové síti připojí.

c) **Virtuální privátní síť (VPN).** VPN je metoda, při níž dochází k připojení počítačových systémů pomocí jiné sítě, kdy po ověření totožnosti počítačových systémů a vzájemném rozpoznání, spolu mohou komunikovat jako v rámci privátní sítě. [9,19]

Pomyslným králem všech sítí je Internet. Jedná se o globální decentralizovanou počítačovou síť, která je složena z mnoha menších sítí, které mezi sebou spojuje protokol TCP/IP. [9,19]

Jednoznačným identifikačním prvkem počítačů v prostředí sítě je IP adresa, kterou využívá Internetový protokol (Internet Protocol). Momentálně je nejrozšířenější druh IPv4. Ten používá IP adresy v 32 bitovém rozhraní a zapisuje číslice dekadicky po osmicích bitů. Nyní je z důvodu nedostatku počtu IPv4 adres přecházeno na novější protokol IPv6, ten se liší v tom, že používá 128 bitové adresy, které jsou zapisovány hexadecimálně [19]

Takzvanou fyzickou adresou nazýváme MAC adresu (Media Acces Control). Jedná se o jedinečný identifikační kód, který je přiřazen síťovému zařízení hned při výrobě, ovšem dá se dodatečně změnit nebo podvrhnout. MAC adresa se skládá z 48 bitů a podle uznávaného standardu by se měla zapisovat do třech skupin čtyř hexadecimálních čísel, které jsou od sebe odděleny pomlčkami nebo dvojtečkami. Dnes se ale častěji zapisuje do šesti skupin dvojciferných hexadecimálních čísel, které od sebe taktéž odděluje dvojtečka nebo pomlčka. [19]

Poskytovatele různých služeb v rámci internetu nazýváme zkratkou ISP (Internet Service Provider). Ti se přímo svou vlastní činností podílí na samotném budování internetu. Dříve bylo označení ISP používáno pouze pro společnosti, které zajišťovali připojení k internetu, dnes se k těmto subjektům řadí i firmy, které poskytují i jiné služby v prostředí internetu, jako je služba e-mailu nebo virtuálního uložiště dat. V ČR se nepoužívá pojem ISP, ale označení poskytovatel služby informační společnosti. Směrnice č. 98/34/ES Rady Evropského parlamentu a definuje služby informační společnosti takto: *„službou je jakákoliv služba informační společnosti, to je každá služba zpravidla poskytovaná za úplatu, na dálku, elektronicky a na individuální žádost příjemce služeb“*. [9]

## 2.2 Druhy kybernetické kriminality

### 2.2.1 Sociální inženýrství v kybernetické kriminalitě

Ve většině publikací o sociálním inženýrství se objevuje výrok Alberta Einsteina *„pouze dvě věci jsou nekonečné, vesmír a lidská hloupost, ačkoli tím prvním si nejsem jist“*. Sociální inženýrství totiž necílí na technickou stránku zabezpečení, ale vybírá si jeho nejslabší článek, a tím je člověk neboli uživatel. Vzhledem k faktu, že žádný počítačový systém není plně autonomní a musí ho řídit lidský subjekt, jeví se jako nejjednodušší cesta získání informací právě od něj.

Sociální inženýrství můžeme rozdělit na dva druhy, které jsou velice často kombinovány. První variantou je sběr veřejně dostupných dat o cíli. Tato varianta v dnešním světě, kdy lidé sdílí na sociálních sítích, jakou technologii používají, kde a kdy jsou, s kým se stýkají apod., dostává úplně jiné rozměry. Není vůbec složité z těchto informací složit příběh nebo vytvořit situaci, kdy dostanu z cíle kýžené informace, například díky podvodnému emailu nebo telefonátu. Druhou variantou je fyzický útok, při kterém se útočník vydá konfrontovat cíl v reálném světě, například jako servisní pracovník, a snaží se získat co nejvíce informací. [9, 16, 20]

V roce 2003 Computer Security Institute ve spolupráci s FBI provedl studii, ve které zjistil, že 77 % společností uvedly nespokojeného zaměstnance jako zdroj závažného prolomení bezpečnosti. Firma Symantec, přesněji její sekce pro prevenci ztráty dat Vontu, zveřejnila report, který říká, že jeden z pěti set emailů obsahuje citlivá data. Tento report také říká, že 62 % nahlášených incidentů může vyústit v krádež identity zakázníků, 66 % pracovníků firem říká, že největším rizikem úniku informací jsou jejich kolegové, nikoliv hackeři. 46 % zaměstnanců uvádí možnost odstranění citlivých údajů z jejich firemního systému jako „snadné“ až „extrémně snadné“ a 32 % zaměstnanců nezná vnitřní směrnice společnosti o ochraně jejich dat. V tomto světle je tedy nejrizikovější částí každého systému uživatel. V případě velkých firem, kdy má do systému přístup velké množství zaměstnanců různých kvalifikací a často s nepříliš vysokou znalostí problematiky IT, se tak jeví jako nejlepší zabezpečení kvalitní proškolení všech uživatelů s přístupem do systému. [20]

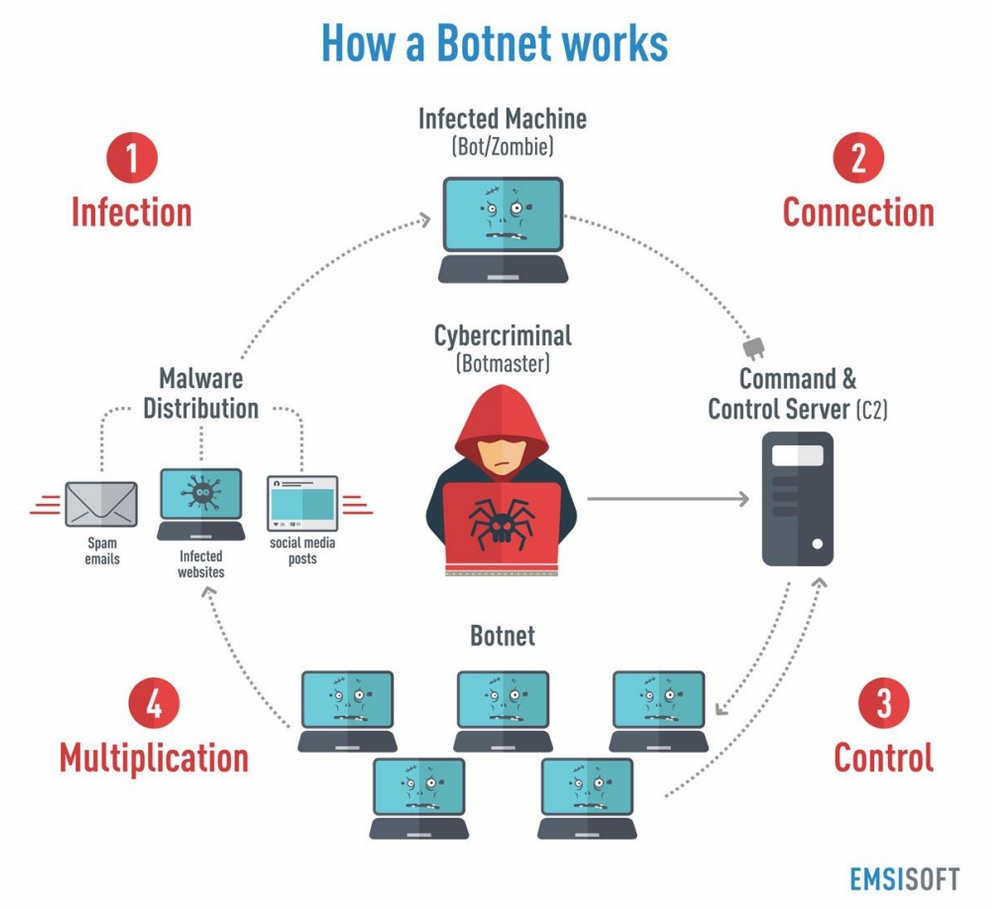
### 2.2.2 Botnet

Výraz botnet je složenina slova Bot (robot) a net (síť) a odkazuje na síť infikovaných zařízení, která jsou pod kontrolou lidského operátora zvaného „botmaster“. Tyto sítě infikují zranitelná zařízení pomocí malware (škodlivý software) skrze spamy (nevyžádaná pošta), infikované webové stránky nebo jsou

součástí neověřených programů, které si uživatel do svého zařízení sám nainstaluje a následně se infikované zařízení připojí k řídícímu serveru (C&C – Comand and Control), přes které je pomocí standardních komunikačních kanálů botmaster ovládá. Sítě botnet využívají zlomek výpočetní kapacity infikovaného zařízení k provádění úkolů, které jim botmaster zadá. Při dostatečné rozsáhlé síti tak vzniká výpočetní potenciál superpočítačů. [21]

Botnet se rozděluje dle architektury, a to na centralizovanou a decentralizovanou síť. Centralizovaná architektura pracuje na principu komunikace klient-server, kdy boti komunikují přímo s řídícím serverem a vykonávají jeho instrukce a využívají jeho zdroje. Oproti tomu botnet s decentralizovanou architekturou je budován na P2P principu, kdy si boti vzájemně své zdroje sdílí a není zde žádný centrální řídící prvek. Takové sítě jsou díky tomu mnohem odolnější vůči pokusům o převzetí kontroly jiným botmasterem. [9]

Infikované zařízení je nejčastěji využíváno k rozesílání spamu, malware, adware, ransomware (druhy malware), phishingových emailů, těžbě virtuálních měn, získávání citlivých informací k dalšímu využívání v rámci krádeže identity nebo organizaci DoS a DDoS útoků vůči systému zvoleném botmasterem. [9]




*Obrázek 2 Jak funguje botnet. [22]*

### 2.2.3 Malware

Malicious software (škodlivý software) neboli zkráceně malware je označován jako kód nebo program, jehož úkol je pracovat v neprospěch hostitelského počítačového systému. Šíření malware probíhá pomocí přenosných paměťových médií (CD, USB, externí disky), stažením infikovaného souboru z internetu a jeho spuštěním, např. souborů s koncovkou doc nebo docx, které obvykle zneužívají zranitelností v daných OS nebo aplikacích, pomocí kterých jsou otevírány a poté se teprve dostane malware do systému. Nejčastěji povolením maker, kdy se následně stáhne externí obsah z internetu – již obsahující škodlivý kód, jako příloha v emailu nebo může být součástí navštívené webové stránky. Malware může mít mnoho podob a plnit různé úkoly. Jeden malware může vykonávat vícero činností, na základě kterých byly druhy malware historicky pojmenovány. [9]

- **Adware** je program, který má za úkol uživateli napadeného zařízení zobrazovat reklamní sdělení v podobě vyskakujících oken v operačním systému nebo jako součást navštěvovaných webových stránek. Tento druh malware je pro systém nejméně škodlivý, avšak velice finančně výnosný a bývá spojen i se spyware.
- **Spyware** neboli „špiónský program“ má za úkol sledovat činnosti uživatele napadeného zařízení a odesílat statistická data zpět k útočníkovi. Spyware může být naistalován jako samostatný malware, ale je často i součástí ověřených a bezpečných programů, kdy uživatel na základě souhlasu smluvních podmínek (EULA) užívání programu souhlasí se zpětným odesíláním dat zpět k výrobci programu. Tato data pak mohou použita například k cílené reklamě.
- **Viry** jsou programy nebo kódy, které se připojí k jinému spustitelnému souboru a po spuštění takového souboru se sami replikují. Existuje celá řada virů, jejichž úkolem může být usídlení v co největším počtu zařízení a jejich následné využití k cílenému útoku nebo ničení dat v infikovaném prostředí, kdy může dojít i ke kompletní destrukci systému. Projevy virů ale mohou být i neškodné, jako například opakované otevírání CD mechaniky nebo spouštění zvuku.
- **Červi** bývají taktéž označovány za viry, ovšem rozdíl mezi červem a virem je v tom, že červ nepotřebuje ke své reprodukci žádný spustitelný soubor. V napadeném systému se sám reprodukuje a rozesílá se na ostatní zařízení, které jsou mezi sebou propojena, což může vést k zahlcení celé sítě. Na rozdíl od virů červi umí analyzovat bezpečnostní slabiny systému a bývají tak využívány k jejich hledání.
- **Trojské koně** jsou programy, které obsahují skryté části, o kterých uživatel neví. Trojské koně tak mohou být buď připojeny k jinému programu nebo mohou být samy vydávány za neškodný program, který si uživatel do svého zařízení naistaluje. Trojský kůň může být využíván

ke kopírování dat nebo narušování funkce systému. Některé trojské koně mají funkci backdoor (zadní vrátka), kdy po spuštění usnadňují přístup dalším škodlivým programům nebo umožňují ovládání systému útočníkem.

- **Rootkit** je technologie sloužící k maskování malware v napadeném systému. Rootkity nejsou škodlivé, mění chování systému, programů nebo aplikací tak, aby se uživatel nedozvěděl, že je jeho systém nakažen malwarem. Napadají i bezpečnostní programy, které mají za úkol hledat malware neboli antivirové softwary.
- **Keylogger** zaznamenává přihlašovací údaje k různým účtům pomocí zaznamenávání konkrétních stisků kláves. Získané informace jsou pak zasílány útočníkovi.
- **Ransomware** je malware, který vydírá uživatele napadeného systému. Existují dva druhy ransomware. První omezí funkčnost celého počítačového systému a uživateli tak není umožněno zařízení vůbec používat, druhý ponechá počítačový systém funkční, ale uzamkne a znepřístupní uložená data. Útok probíhá tak, že jakmile se počítač ransomwarem infikuje, zpravidla se zobrazí na obrazovce hlášení, které se vydává za policii nebo jinou důležitou instituci, obviňuje uživatele ze spáchání nějaké trestné činnosti (sledování dětské pornografie, počítačové pirátství) a požaduje zaplacení určitého obnosu k obnově funkcí systému. Po zaplacení ovšem často k odblokování zařízení ani nedojde. Pro ransomware je typické, že často používá velice lámanou češtinu, špatný výběr grafiky pro danou instituci (znak apod.) a nevzhledné zpracování. V průběhu času se ovšem tvůrci ransomware díky technice sociálního inženýrství zdokonalují a jejich programy jsou pro laika hůře odhalitelné. [9]

### 2.2.4 Spam

Jako spam označujeme veškeré nevyžádané zprávy, které jsou šířeny pomocí internetu. Nejčastěji to jsou reklamní sdělení, která jsou adresátovi doručována v podobě elektronické pošty, může k tomu být ovšem také využita jiná komunikační platforma, jako například SMS, Skype nebo sociální sítě. Činnost spočívající v rozesílání těchto nevyžádaných zpráv se jmenuje spamming. Spammeři získávají emailové adresy nejrůznějšími způsoby. Zdrojem jsou například jakékoliv webové stránky, kde jsou dostupné emailové schránky registrovaných uživatelů. [9, 16]

Statisticky je více než polovina odeslaných emailů spam. Největší podíl měl spam v březnu roku 2014 a to 71,1 %. V březnu a dubnu roku 2018 poprvé po dlouhé době klesl podíl spamu v elektronické poště pod 50 % a to na 48 %. Vezmeme-li v potaz, že se v roce 2018 odeslalo 281 mld. emailů, činí tak nevyžádaná pošta v průměru více než 140 mld. zpráv ročně. Uživatel, který obdrží spam má možnost nahlásit emailovou adresu, ze které tento email přišel, například na webových stránkách www.spamcop.cz, jejíž zřizovatelé následně tyto adresy předávají internetovým poskytovatelům. [23, 24]

Spam, který obsahuje kriminální nebo podvodný obsah se označuje jako scam. Scamy využívají sociálního inženýrství, aby v adresátovi vzbudili jeho důvěru a donutili ho tak udělat kroky, které po něm vyžadují. Mezi scamy můžeme zařadit phishing, malware, hoaxy nebo podvodné loterie. [9]

### 2.2.5 Phishing a jeho formy

Phishing je forma sociálního inženýrství, kdy se útočník snaží získat důvěru tím, že se vydává za důvěryhodnou osobu nebo instituci a snaží se z oběti vylákat důvěrné informace, jako například přihlašovací údaje do elektronického bankovnictví, číslo kreditní karty, PIN apod. V obecné rovině se ovšem dá za phishing považovat jakékoli podvodné jednání, které má za úkol donutit oběť

akceptovat předem připravený scénář a nemusí jít tak ani o získávání přihlašovacích údajů apod. [9]

Phishingový útok probíhá v několika krocích. První z nich je naplánování takového útoku a vytvoření scénáře, který útočník chce, aby oběť akceptovala. Se scénářem se také musí určit skupina obětí, kterou má daný scénář největší šanci obelhat. V další fázi dochází k technickému řešení útoku, jako vytvoření stránky a důvěryhodného sdělení k získání požadovaných informací. Současně je zapotřebí získání kontaktů na budoucí oběti útoku. Třetím krokem je samotný útok, kdy je phishingový email doručen oběti. V tomto kroku útok buď skončí tím, že oběť odhalí nebo útočníkovi požadované informace poskytne. Následně útočník získává data od oběti a v poslední fázi pomocí získaných informací dojde k odčerpání finančních prostředků nebo získání jiného profitu, za kterým byl útok veden. [9]

Pharming je sofistikovanější forma phishingu, který cílí na DNS server, kde dochází k překladu doménového jména na IP adresu. Uživatel tak zadá do prohlížeče adresu webové stránky, na kterou se chce přihlásit, ovšem zobrazí se mu falešná webová stránka, často nerozeznatelná od té originální, a dojde tak k získání přihlašovacích údajů. Tato forma bývá nejčastěji používána u internetového bankovnictví. [9]

Spear Phishing je na rozdíl od klasického phishingu, který je směrován plošně na velkou skupinu potencionálních obětí, cílen přímo na jednotlivce, úzkou skupinu lidí nebo organizaci. Útočník získá z otevřených zdrojů co nejvíce informací o oběti a vytvoří scénář přímo na míru. [9]

Jako vishing se označuje telefonická forma phishingu. Tak jako v předchozích formách se i zde využívá značná míra sociálního inženýrství a útočníci tak mohou vystupovat jako zástupci banky oběti a získat tak citlivé informace k získání finančních prostředků z účtu oběti. Phishing pomocí SMS zpráv se jmenuje

smishing a útočník se většinou snaží donutit příjemce buď odeslat DMS nebo zavolat na jinou placenou linku. [9]

V roce 2005 proběhla na Indiana University studie, kdy byla vybrána skupina 349 studentů ve věku 18-24 let, kteří o sobě sdělovali na internetu dostatečné množství informací a byli tak mnohem více náchylnější k tomu, aby byli útočníkem vybrány k jeho phishingovému útoku. Těmto studentům byl následně odeslán email z adresy s univerzitní doménou, který obsahoval text „Hey, check this out!“ a odkaz na falešnou stránku s nutností zadání přihlašovacích údajů do univerzitního systému. Své přihlašovací údaje pak vyplnilo 72 % studentů. Kontrolní skupina 96 studentů pak obdržela stejný email, ovšem odeslaný z neznámé adresy, a i přesto přihlašovací údaje vyplnilo relativně vysokých 16 % studentů. [25]

### 2.2.6 Hacking

Od samých začátků počítačů byli hackeři lidé, kteří se snažili kreativně řešit problémy. Dnes je pojem „hacker“ veřejností vnímán spíše negativně, jako člověk, který se snaží nelegálně získat přístup do cizího počítačového systému nebo ho nějakým způsobem poškodit. Počátky hackerů datujeme do pozdních padesátých let, kdy klub železničních modelářů na MIT získal darem součástky telefonního vybavení a tyto součástky následně použili k vytvoření systému, kterým ovládali model železnice pomocí vytáčení čísel. Tuto techniku nazvali „nové a inventivní použití telefonního hackování“. Následně se modeláři přesunuli k programování mechanických počítačů jako IBM 704. Jejich cílem bylo psát programy tak, aby používali co nejmenší počet děrovaných karet, na kterých tehdejší počítače pracovali. Tato skupina je dnes považována za první originální hackery. [26]

Hackování se tím posunulo do jisté formy umění a stejně jako řada ostatních forem umění bylo často nepochopeno. Hackeři v dalších letech chtěli po novinářích, aby osoby, které nerespektují zákony v kybernetickém světě a páchají trestnou činnost byli nazýváni názvem „cracker“, ten se ovšem neujal. Ti, kteří se

stále chtěli zdokonalovat v hackování věřili, že veškeré informace by měly být všem dostupné a jestliže se objevila překážka, která to znemožňovala, musí být obejita. Ve světě hranic se tak tyto neoficiální skupiny hackerů rozhodli následovat vědění samotné, namísto konvenčních cílů vzdělávání. Chtěli vytvořit místo bez zbytečné byrokracie, zakazujících autorit a diskriminace. V tomto duchu například výše zmiňovaný klub modelářů přijmul do svých řad 12-ti letého chlapce, který prokázal znalosti v programovaní a touhu po dalším učení. Nic takového jako věk, rasa, pohlaví nebo sociální postavení nehrálo roli v posuzování práce v hackerském prostředí. [26]

I dnes stále platí, že hacker je osoba, která má vynikající znalosti v oblasti programování a informačních technologií. Na základě jejich primární motivace vytvořit nestandardní řešení nebo průnik, avšak ne nutně nelegální, rozdělujeme hackery do tří hlavních skupin.

- White Hats – je skupina hackerů, která proniká do systémů z důvodu hledání slabin v jejich zabezpečení a jejich následném odstranění. Důležité je, že samotným průnikem do systému nepůsobí škody a nezískají z něj žádný prospěch mimo odhalení slabin zabezpečení. Následně upozorní správce sítě na mezery v zabezpečení.
- Black Hats – jedná se o opak white hats. Jejich motivací a cílem je způsobení škody nebo získaní vlastního profitu z průniku do systému. V rámci realizace průniku je současně zřejmý další kriminální prvek.
- Grey Hats – jsou hackeři, kteří se nevyprofilovali do ani jedné z výše uvedených skupin. Občas v jejich jednání může dojít k porušení zákona, ale primární motivací jejich činů není způsobení škod nebo získání osobního prospěchu. [9]

Hackeři ve svých činnostech využívají různé techniky. Mezi typické druhy činností hackerů můžeme zařadit:

- Sociální inženýrství.
- Prolamování hesel.
    - Útok hrubou silou, kdy dochází k testovaní znakových kombinací.
    - Hádaní hesla na základě znalostí o uživateli.
    - Využití slovníku nejčastěji používaných hesel.
    - Vydávání se za uživatele, při pokusu obnovy hesla pomocí administrátora sítě.
    - Odchytávání hesla z nechráněné komunikace.
    - Hledání hesel uložených v datech systému.
- Skenování portů – na základě skenování otevřených síťových portů lze určit, jaké služby jsou na počítačovém systému zrovna spuštěny.
- Využívání malware k infiltraci počítačového systému.
- Phishing.
- Cros Site Script – jedná se o útok pomocí skriptů, ve kterém je vložen závadný kód, který je umístěn na narušených webových stránkách.
- Odposlech komunikace. [9]

### 2.2.7 Cracking

Cracking je přímo spjat s počítačovým pirátstvím a hackováním. V principu se jedná o obcházení bezpečnostních mechanismů, které zabraňují neoprávněnému užívání a kopírování. Primárně se cracking týká softwaru všeho druhu, od celých operačních systémů přes photoshopy až po videohry. Asi nejrozšířenější metodou je „reverse engineering“, kdy hacker provádí zpětnou dekompilaci programu a umožní tak obejít ochranu hardwarového klíče. Hackery, kteří provádí cracking, řadíme mezi Black Hats, jelikož zde dochází porušování autorského práva. [27]

### 2.2.8 Počítačové pirátství

Počítačové neboli internetové pirátství je pojem, který pod sebou zastřešuje veškerou kriminalitu vztahující se k právům duševního vlastnictví. S rozvojem

osobních počítačů a internetu je počítačové pirátství masovou záležitostí a jedním z nejrozšířenějších projevů kybernetické kriminality. [9]

**Autorský zákon**

Výsledkem tvůrčí činnosti člověka mohou být nehmotné statky spadající do oblasti duševního vlastnictví. Právo duševního vlastnictví je nezávislé na hmotném substrátu a může být užíváno kdykoli a kdekoli na světě za podmínky, že je jedinečné, neopakovatelné a dostatečně originální. [9]

Hlavním právním předpisem upravující oblast autorského práva je v České republice zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění dalších předpisů. Tento zákon v sobě zahrnuje všechny příslušné předpisy Evropské unie.

V § 1 autorský zákon upravuje:

***a)*** práva autora k jeho autorskému dílu,
***b)*** práva související s právem autorským:
- ***1.*** práva výkonného umělce k jeho uměleckému výkonu,
- ***2.*** právo výrobce zvukového záznamu k jeho záznamu,
- ***3.*** právo výrobce zvukově obrazového záznamu k jeho záznamu,
- ***4.*** právo rozhlasového nebo televizního vysílatele k jeho vysílání,
- ***5.*** právo zveřejnitele k dosud nezveřejněnému dílu, k němuž uplynula doba trvání majetkových práv,
- ***6.*** právo nakladatele na odměnu,

***c)*** právo pořizovatele k jím pořízené databázi,
***d)*** ochranu práv podle tohoto zákona,
***e)*** kolektivní správu práv autorských a práv souvisejících s právem autorským (dále jen „kolektivní správa“). [28]

V § 2 autorský zákon vymezuje pojem dílo, jenž definuje jako *„dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě včetně podoby elektronické, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam“. [28]*

Dále autorský zákon stanovuje, že se vztahuje na *„dílo dokončené, jeho jednotlivé fáze vývoje a části, včetně názvu a jmen postav, pokud splňují podmínky podle odstavce 1 nebo podle odstavce 2, jde-li o předměty práva autorského v něm uvedené“* [28] a upravuje, že dílem je zejména:

- Dílo slovesné vyjádřené řečí nebo písmem (proslov, kniha, scénář).
- Dílo hudební (hudební skladba).
- Dílo dramatické a dílo hudebně dramatické (divadelní představení, muzikál, opera).
- Dílo choreografické a dílo pantomimické (balet, tanec).
- Dílo fotografické a dílo vyjádřené postupem podobným fotografii (fotografie).
- Dílo audiovizuální, jako je dílo kinematografické (film, animovaný film).
- Dílo výtvarné, jako je dílo malířské, grafické a sochařské (malba, črta, kresba, animace, socha, grafika).
- Dílo architektonické včetně díla urbanistického (stavba).
- Dílo užitého umění a dílo kartografické (mapa, atlas).
- Počítačový program.
- Dílo souborné (sborník, časopis, encyklopedie, antologie, pásmo, výstava). [28]

V šestém odstavci § 2 pak autorský zákon říká, že dílem dle autorského zákona není *„námět díla sám o sobě, denní zpráva nebo jiný údaj sám o sobě, myšlenka, postup, princip, metoda, objev, vědecká teorie, matematický a obdobný vzorec, statistický graf a*

*podobný předmět sám o sobě“*. Podle § 3 se autorský zákon nevztahuje na úřední dílo (právní předpisy, veřejný listiny apod.), výtvory tradiční lidové kultury (není-li pravé jméno autora obecně známo) a státní symboly (viz. Zákon č. 352/2001 Sb., o užívání státních symbolů České republiky a o změně některých zákonů). [28]

**Projevy počítačového pirátství**

Okruhu lidí, který vypouští do světa internetu díla k volnému šíření se také říká „warez“ scéna. Jedná se o Black Hats hackery a jejich činnost se skládá hlavně z crackingu a následné distribuce svého cracku na fórech a www stránkách v kombinaci s reklamou nebo odkazy s žádostmi o dobrovolné finanční dary na provoz skupiny, čímž je zajištěn finanční profit z činnosti, samotný produkt je k dosažení zdarma. Výsledný vydaný produkt se nazývá Release. Pirátství se tímto způsobem dotýká téměř všech druhů děl. Mezi nejznámější skupiny šířící realese, se řadí SKiDROW, RELOADED nebo například Razor1911. [27]

Druhou variantou stahování jsou tzv. torrenty. Fungují na principu P2P sítě, kdy za pomoci programu (µTorrent, BitTorrent) dochází ke stahování a odesílání fragmentů požadovaného souboru od ostatních uživatelů. Torrent se říká prvnímu souboru, který se nahraje do programu. Tento soubor obsahuje metadata o sdílených datech a tracker požadovaného souboru, který je uložen u ostatních uživatelů. Uživatelům připojeným na jeden tracker, který data stahuje, se říká „peers“, ti co stahují, se nazývají „leachers“ a uživatel, který je odesílá se nazývá „Seeder“. V procesu stahování je zpravidla uživatel leacher a seeder zároveň a poskytuje jím stažená data ostatním peerům. Výhodou této technologie oproti stahování z uložišť je vysoká rychlost při nulových nákladech, nulová cenzura (provozovatelé uložišť na základě podané žádosti soubory porušující autorský zákon mažou), avšak jestliže uživatel nestahuje pomocí VPN, je internetovými providery, kteří tento druh aktivity ve své síti sledují, velice snadno dohledatelný.

Dále je možné díla šířit pomocí emailu (tato varianta je ale díky nízké přenosové kapacitě hůře využitelná), na vlastních webových stránkách (lze šířit pouze soubory o malé velikosti a tato forma je velice brzy odhalena a zablokována) a jako poslední možnost je fyzický přenos pomocí CD, DVD nebo flash disků. [9]

Studie evropské unie s názvem „Estimating displacement rates of copyrighted content in the EU“ z roku 2015, ve které bylo 30 000 zákazníků dotazováno o nákupu a ilegálním stahování videoher, sice z velké části spoléhá na data o nákupu a ilegálním stažení, ale ptá se respondentů také na otázky typu, kolik by byli ochotni zaplatit za jejich poslední ilegálně staženou hru a zjišťuje jejich morální postavení k ilegálnímu stahování. Bylo zjištěno, že na každých 100 ilegálně stažených her jich je zakoupeno 24 navíc. Tento pozitivní efekt ilegálně stažených her a streamingu spočívá v tom, že společnosti jsou schopny z pirátů pomocí bonusových služeb, obsahu a kvality vytvořit hráče platící. [28]

### 2.2.9 Sniffing

Sniffing je metoda odposlouchávání dat při komunikaci na počítačové síti pomocí programu zvaného „sniffer“, neboli čichač. Tento sniffer odchytává pakety, které jsou následně analyzovány. Tato technika se používá standardně administrátory sítí pro diagnostiku anomálií v provozu. V případě, že tato činnost probíhá za cílem správy sítě, není nelegální. Jakmile ovšem administrátor během této činnosti využije jakýkoliv program k záchytu komunikace nebo bez vědomí uživatele sleduje jeho emailovou nebo hlasovou komunikaci, aby mohl získaná data nadále zneužít ve svůj prospěch a způsobit tak uživateli škodu, jedná se o trestný čin § 182 trestního zákoníku – porušení tajemství dopravovaných zpráv. [9]

Dopadení pachatele, který provádí sniffing a následné dokázání této činnosti je ovšem téměř nemožné a výše uvedená trestní klasifikace je tak spíše hypotetická. Jinak by to ovšem bylo v případě, že by soukromý subjekt konstantně odposlouchával jiný soukromý subjekt a získaná data by následně použil v krocích

proti němu. Takovéto akce samy o sobě vyvolávají otázky, kde a jak se k takovým datům ostatní subjekty dostaly. [16]

### 2.2.10 DoS, DDoS, DRDoS útoky

DoS je zkratkou pro Denial of Service, v překladu odmítnutí služby. Princip tohoto útoku je cílený počítačový systém či prvky sítě zahltit úkony, které mají vykonat. Při dostatečném přetížení dojde ke zpomalení služby a následně i ke kolapsu sítě či počítačového systému. Toto zpomalení nebo dočasné vyřazení je zároveň i cílem útoku. Existuje několik forem provedení útoků tohoto ražení. [9]

DoS útok je základní variantou a probíhá z jednoho zdroje. Tento typ útoku jde poměrně snadno odrazit blokováním provozu z daného zdroje útoku. [9]

DDoS (Distributed Denial of Service) probíhá stejně jako DoS varianta, ovšem útočník nebo útočníci provádí útok z většího množství zdrojů. Při menším počtu se dá znovu zablokovat provoz ze zdrojů útoku, ovšem při větším množství útočníků, například při použití botnetu nebo při útoku s kampaní, například od skupiny Anonymous, která má poměrně širokou základnu a podporu počítačové veřejnosti, dosahují zdroje útoku vysokých počtů a je téměř nemožné tuto variantu obrany uplatnit. [9]

DRDoS (Distrubuted Reflected Denial of Service) využívá tzv. mechanismu odražení. Samotný útok probíhá tak, že zdroj útoku vyšle velké množství požadavků, ale ne na oběť útoku. Tyto požadavky míří na ostatní počítačové systémy, kdy jako zdroj požadavku, který tyto systémy obdrží, je uvedena oběť útoku. Počítačový systém, který je obětí, pak dostává velké množství odpovědí, které si vůbec nevyžádal a od systému, které nevědí, že jsou součástí útoku. [9]

Existuje několik metod jak DoS nebo DDoS útoky provést. První takovou metodou je využití vlastností síťových mechanizmů, a to především protokolu

ICMP (Internet Control Message Protocol). Tento protokol dokáže zjistit existenci počítače s danou IP adresou pomocí příkazu ping. Jestliže se ovšem pošle ping na adresu sítě, odpoví všechny počítače dané sítě. Útok probíhá tak, že se příkaz ping odešle do sítě se změněnou adresou odesílatele a oběť se stane zahlcená odpověďmi na odeslaný příkaz ping. [16]

Další variantou je zahlcení pakety SYN. Paket SYN se používají v protokolu TCP pro sestavení spojení. Jakmile systém obdrží paket SYN, odešle na ni odpověď a dál čeká na potvrzení spojení. Čekání na toto potvrzení může trvat v řádech minut. Jestliže útočník během tohoto času odešle dostatečný počet paketů a vyčerpá volné kapacity systémových prostředků, systém není schopen realizovat spojení pro potvrzení a stává se nedostupným. [16]

K realizaci útoku DRDoS se používá technika zvaná IP Spoofing. Jedná se o falšování zdrojové adresy, kdy útočník zadá do paketu zdrojovou adresu oběti a ne svou. Tímto způsobem odešle pakety na velké množství okolních systémů, které pak zahltí oběť odpověďmi na požadavek, který neodeslala. [9]

V roce 2018 byl dvakrát v rozmezí pěti dnů překonán světový rekord ve velikosti DDoS útoku. 28. února webová stránka www.github.com přežila DDoS útok, kdy během 8 minut zaznamenala provoz o velikosti 1,3 Tbps, kdy standardní vytížení této vývojářské platformy je okolo 100 Gbps. [29] Jen o pět dní později neznámý provozovatel telekomunikační sítě se sídlem v USA zaznamenal masivní vytížení, které dosahovalo až k 1.7 Tbps. Předchozí rekord z roku 2016 byl útok na webové stránky televizní stanice BBC, kdy došlo k jejich vyřazení a maximální zatížení dosáhlo 602 Gbps. [30]

### 2.2.11 Kybernetická kriminalita na sociálních sítích

V prostředí sociálních sítí se dá dělat většina výše popsané kybernetické kriminality (šíření malware, pirátství, phishing, atd.). Samostatně budou popsány druhy kybernetické kriminality, které jsou specifické pro prostředí sociálních sítí.

**Internetový trolling**

Internetoví trollové vkládají na internetu velice urážlivé a pobuřující příspěvky s cílem vyprovokovat ostatní uživatele. Tyto komentáře se objevují na různých fórech nebo diskuzích pod internetovými články (například články zveřejněné na zpravodajském portálu www.novinky.cz spojené s migrační vlnou mívají po několika desítkách minut zablokovanou možnost komentovaní, právě kvůli těmto uživatelům). S rozmachem sociálních sítí se jejich činnost a počet rapidně zvýšily. Příspěvky těchto uživatelů často obsahují vyhrožování smrtí či fyzickým násilím nebo sympatizování a podporu genocidy. [31]

Na českém internetu se s podobným jednáním setká uživatel téměř denně. Známá je kauza, kdy facebooková stránka WeAreHereAtHome (My jsme tady doma), která během převzala fotku malého Ibrahima Kary z pravidelného tabla čerstvě narozených novorozenců ve Frýdecko-Místeckém deníku, protože má Kurdského otce. V komentářích se pak doslova strhl souboj o to, kdo bude autorem nejodpornějšího příspěvku. [32]

Týdeník Respekt následně vyhledal autory těchto příspěvků, aby se jich zeptal, co je vedlo k tomu, že takové věci psali na adresu novorozence. Jozef Karban, který pod fotku napsal „okamžitě utopit“, odpověděl, že zrovna přišel domů z hospody, měl upito a nechal se strhnout. [32] Řada ostatních komentářů se už dostala do hledáčků policie a dva účastníci debaty za ni již byli odsouzeni. Pavel Hrabák byl za příspěvek „Je to odpad, má to v genech. Bude se jen dál množit, kolik takovej negr bude mít za 25 let potomků. Takže za mě, dupnout na krk,“ odsouzen

trestním příkazem ke 100 hodinám veřejně prospěšných prací podle § 356 trestního zákoníku za podněcování k nenávisti vůči skupině osob nebo omezení jejich práv a svobod. Druhou odsouzenou je Lada Vyskočilová, která byla za komentář „Nemá tady co dělat, já být porodník, mám za dopoledne plnej kýbl“ odsouzena k trestu odnětí svobody v délce jednoho roku s podmíněným odkladem výkonu trestu na čtyři roky. [33]

**Kyberšikana a sexting**

Kyberšikana je chování, které v sobě zahrnuje vyhrožování, ohrožování, ponižování a jiné negativní projevy jednotlivce nebo skupiny vůči jiným jednotlivcům nebo skupinám za použití informačních technologií. Tato forma šikany se může navzájem prolínat s „klasickou“ šikanou. Typologicky kyberšikanu rozdělujeme do několika skupin: [34]

- „Vytáčení“ – On-line „boje“ prostřednictvím elektronických zpráv s využitím vulgárního jazyka. Ekvivalent silové agrese.
- Obtěžování – Opakované zasílání urážlivých a hanlivých zpráv. Ekvivalent přímé šikany.
- Kybersledování – Záliba v on-line aktivitách, které způsobují jednotlivci strach o svou bezpečnost.
- Očerňování – Posílání nebo zveřejňování hrubých pomluv nebo osočování s cílem zničit pověst mezi přáteli.
- Používání druhé identity – Vydávání se za jinou osobu ve snaze oběť znemožnit nebo poškodit její pověst nebo přátelství.
- Odhalovaní tajemství – On-line zveřejňování tajemství, hanobících informací nebo obrázků jiné osoby.
- Používání lži a podvodů – Zmanipulování osoby tak, aby odhalila hanobící informace a jejich následné sdílení.
- Vyloučení – Záměrné vyloučení člověka z on-line skupiny [34]

Mezi znaky kyberšikany je možné zařadit:

- Pocit anonymity.
- Neomezenost útoku.
- Neomezený okruh útočníků.
- Neomezený prostor a prostředky.
- Obtížná zjistitelnost.
- Trvalost. [9]

Oběti kybernetické šikany mohou skončit stejně fatálně jako oběti běžné šikany. Často končí sebevraždami nebo nutností psychologické pomoci. Výše uvedené znaky kybernetické šikany ukazují, že je mnohem těžší ji zastavit. Kyberšikanu je v ČR možné klasifikovat jako trestný čin v případě vygradování k fyzickému útoku jako § 146 (Ublížení na zdraví) nebo v jiných případech § 175 (Vydírání) a § 354 (Nebezpečné pronásledování).

Sexting je forma elektronické komunikace, jejímž obsahem jsou texty, videa nebo obrázky se sexuálním obsahem. Tato forma komunikace se dá rozdělit do dvou druhů, dobrovolné a nátlakové. Jako dobrovolnou formu sextingu považujeme zasílání erotického obsahu mezi jednotlivci, kteří tak chtějí uspokojit svou sexuální zvědavost. Také může představovat způsob sblížení mezi dvěma osobami, nebo se jedna osoba snaží přilákat pozornost druhé. Nátlaková forma sextingu pak zahrnuje zasílání erotického obsahu obětí útočníkovi pod nátlakem, například vydíráním nebo vyhrožováním. Získaný materiál dobrovolného i nátlakového sextingu pak může být využit k vydírání nebo vyhrožování oběti zveřejněním na internetu. [34]

**Kyberstalking**

Kyberstalking je nevhodné chování, které se projevuje zejména opakovaným a dlouhodobým kontaktováním a sledováním jiné osoby pomocí internetu. Může se

prolínat i s normálním stalkingem, kdy probíhá i fyzické sledování a kontaktování mimo svět internetu, například dopisy nebo telefonními hovory. Sociální sítě jsou také využívány k stalkování celebrit. V roce 2015 osoba vystupující pod jmény Alex Mercer a Ralph Alexander zveřejnila obrázky brokovnice a sebe před bydlištěm zpěvačky Rihanny s popiskem, že ji měl radši zavraždit. [31] V ČR takové jednání lze klasifikovat jako tr. čin Nebezpečné pronásledování dle ust. § 354 trestního zákoníku. Uvedené ustanovení v sobě zahrnuje všechny formy pronásledování.

### 2.2.12 Šíření dětské pornografie a nenávistného obsahu

Mezi závadový obsah, který se momentálně šíří na internetu, řadíme druhy zakázané pornografie a nenávistná a extrémistická sdělení. [9]

Problém zacházení s dětmi jako se sexuálními objekty existuje od nepaměti a s tím i související vytváření a distribuce materiálů zobrazující takovéto jednání. Před nástupem internetu, kdy distribuce dětské pornografie probíhala na fyzických médiích (papír, film) měli bezpečnostní složky poměrně velký úspěch při vyhledávání a ničení takového materiálu. Nicméně se spuštěním internetu se tato problematika poměrně zkomplikovala a bezpečnostní složky tak musely začít jiným způsobem vyšetřovat a kontrolovat tento jev. [35]

Internetová dětská pornografie se rozděluje do tří částí. Produkce, distribuce a stahování.

Produkce zahrnuje vytváření pornografického obsahu. Ačkoliv některý materiál může být desítky let starý a pouze převeden ze starších fyzických médií jako je papír a film, značná část současného obsahu je tvořena amatérsky pomocí webových kamer nebo jiných tomu podobných elektronických zařízení. [35]

Distribuce dětské pornografie je zejména upload a rozesílání na internetu. K tomu pak může sloužit forma přenosu server-klient, klient-klient (P2P), email

nebo například vlastní webové stránky na kterých je obsah dostupný. Stopování a ničení materiálu, který je šířen pomocí P2P sítí je problematické, oproti tomu například webové stránky bývají zrušeny okamžitě po jejich objevení. Šíření pomocí emailu je lépe vyhledatelné a uživatel se tak může dostat do povědomí policie. Distribuce těchto materiálů se ve velké míře odehrává na DarkNetu, kde jsou ostatními uživateli sdíleny odkazy kde lze stáhnout dětskou pornografii. [35]

Stahování zahrnuje získání přístupu k dětské pornografii pomocí internetu. Tento přístup nezahrnuje pouze stahování materiálu na vlastní diskové uložiště, ale může se vyskytovat i ve formě internetových přehrávačů nebo například při vyskočení nevyžádaného pop-up okna směřujícího na dětskou pornografii, většinou ovšem musí uživatel sám vědomě vyhledávat takový obsah. Nejvíce takového obsahu se ovšem stahuje skrze chatovací místnosti nebo diskuzní fóra. [35]

I přes obtížnost vyšetřování tohoto druhu kriminality je důležité jejich zapojení a k tomu je zapotřebí hlavně získání technických vědomostí a odborných znalostí v oblasti internetové pornografie, spolupráce s ostatními složkami a agenturami, které jsou v dané problematice zainteresování, být ve spojení s poskytovateli internetu, kteří jim následně pomáhají s vyhledáváním pedofilů a pornografických materiálů. Nakonec je potřeba se při velkém množství dětské pornografie na internetu koncentrovat na větší sexuální delikventy, kteří produkují a distribuují dětskou pornografii. [35]

V případě šíření nenávistných a extremistických sdělení se jedná zejména o podporu hnutí a ideologií, které prokazatelné směřuje k potlačování lidských práv a svobod člověka. Do toho zahrnujeme i projevování sympatií s těmito uskupeními, které se velmi často objevuje na sociálních sítích. Dále se sem řadí šíření pomluv a zasílání obtěžujících zpráv pomocí informačních technologií (stalking, cyberstalking). [9]

### 2.2.13 Krádež virtuální identity

Krádeží virtuální identity (Identity theft) máme na mysli dočasnou nebo trvalou kontrolu či převzetí nad jinou identitou. Důvodem páchání těchto krádeží může být finanční motivace nebo získání přístupu k firemním datům atd., která jsou získána právě v zastoupení ukradené identity. [9]

Útočník při krádeži identity většinou musí provést několik protiprávních jednání naráz. Většinou se tak stává prolomením přístupových údajů nebo instalací malware do počítačového systému oběti kvůli získání přístupu k virtuální identitě. Následně může dojít ke zneužití získaných informací k útoku na osobu, o které útočník informace získal nebo se informace využijí k útoku na jinou osobu, ten je pak o poznání jednodušší, protože druhá oběť netuší, že došlo ke krádeži identity a s útočníkem, jenž vystupuje jako někdo jiný tak ochotně komunikuje. [9]

Odcizené virtuální identity se pak nejčastěji používají k phishingovým nebo malwarovým útokům na ostatní uživatele, se kterými oběť komunikuje, rozesílání spamu, získávání informací, jenž nejsou veřejně dostupné (přístup do firemních systému atd.) a získávání přístupů do dalších služeb jako internetové bankovnictví, účty na sociálních sítích, internetových obchodech atd. [9]

### 2.2.14 Kyberterorismus

Poprvé se fráze kyberterorismu objevila v polovině osmdesátých let. Barry C. Collin, starší výzkumník z Institute for Security and Inteligence v Kalifornii definoval kyberterorismus jako „konvergence kybernetiky a terorismu“. K této elegantní a jednoduché, avšak nedostatečně specifické definici se tak během let přidalo mnoho dalších. Eric Luiijf pak v knize „Cyber crime and cyber terrorism investigator’s handbook“ vytvořil komparaci většiny definic, a definuje kyberterorismus jako: *„Užití, příprava nebo hrozba vytvořená ke způsobení změny veřejného pořádku, způsobení strachu nebo zastrašení většiny (nebo její části) veřejnosti,*

*ovlivnění politických rozhodnutí vlády nebo mezinárodních organizací v prospěch politických, náboženských, rasových či ideologických důvodů díky ovlivnění integrity, důvěryhodnosti, dostupnosti informací, informačních systémů a sítí neautorizovanými činy ovlivňující informačních a komunikačních technologií určených k řízení fyzických procesů reálného světa, které zahrnují nebo způsobují:*

- *Násilí, utrpení, vážná zranění nebo smrt osob.*
- *Závažné poškození majetku.*
- *Závažné ohrožení života a zdraví veřejnosti.*
- *Závažnou ekonomickou ztrátu.*
- *Závažné narušení ekologické bezpečnosti.*
- *Závažné narušení veřejného pořádku, politické stability a soudržnosti státu".* [Volný překlad autora z angličtiny - 36]

Internet dovoluje extremistickým a teroristickým skupinám především rychlou, efektivní a relativně utajovanou komunikaci při přípravě a provádění teroristických činů. Uvádí se, že útok na World Trade Centre v New Yorku již byl organizován s pomocí internetu. Bezmála všechny teroristické skupiny provozují vlastní internetové stránky a internetové prostředí jim tak pomáhá šířit svou propagandu mnohem efektivněji. [9]

## 2.3 Bezpečnostní složky v oblasti kybernetické kriminality

### 2.3.1 Policie ČR

V České republice probíhá vyšetřování běžné kybernetické kriminality na 14 krajských ředitelstvích a jejich územních odborech. Závažnou trestnou činnost v oblasti kybernetické kriminality pak vyšetřuje sekce kybernetické kriminality NCOZ SKPV, která je rozdělena na odbor kybernetické kriminality a odbor vyšetřování kybernetické kriminality. Sekce kybernetické kriminality je zároveň Národním kontaktním bodem pro kybernetickou kriminalitu dle Budapešťské

úmluvy o kybernetické kriminalitě. Zároveň zajišťuje přijímání podnětů z NÚKIB a spolupracuje s Interpolem a Europolem na přijímání poznatků vztahující se k šíření dětské pornografie na internetu. [37]

### 2.3.2 Europol

Europol v boji pro kybernetické kriminalitě v roce 2013 založil European Cybercrime Centre (EC3). EC3 má dva forenzní týmy, které se specializují na forenzní zkoumání digitálních uložišť a forenzní analýzu elektronických dokumentů. Oba se specializují na operativní podporu, výzkum a vývoj. Dále se dělí na dva strategické týmy. První má na starosti aktivní pomoc a podporu, čímž buduje spolupráci a koordinuje opatření pro zvýšení povědomí o kybernetické kriminalitě. Druhý tým se zaměřuje na strategii a vývoj čímž je odpovědný za strategické analýzy, formulaci zásad, legislativních opatření a vývoj standardizovaného tréninku. EC3 se zaměřuje na zločiny související s kybernetickou kriminalitou, zneužívání dětí na internetu a platební podvody. [38]

Souběžně s EC3 pracuje také Joint Cybercrime Action Taskforce (J-CAT), který se soustředí na tu nejzávažnější mezinárodní kybernetickou kriminalitu, jenž zasahuje členské státy Evropské unie a jejich občany. [38]

### 2.3.3 Interpol

Interpol podniká mnoho aktivit pro podporu členských zemí v boji pro kybernetické kriminalitě. Díky časté mezinárodní povaze kybernetické kriminality je Interpol partnerem ve vyšetřování těchto zločinů na kooperativní úrovni. Hlavní činností Interpolu v kybernetické kriminalitě je tak operativní a vyšetřovací podpora, zpravodajská činnost a analýza, výzkum, budování kapacit a vytváření národních kybernetických přehledů. Interpol také provozuje Interpol Global Complex for Innovation, což je zařízení pro vývoj a výzkum v oblasti kybernetické kriminality v Singapuru a zřizuje Interpol Global Cybercrime Expert Group, což je

skupina, která spojuje experty z různých odvětví spojených s kybernetickou kriminalitou a poskytuje rady zahrnující strategii, výzkum, trénink forenzní a operativní činnost. [39]

## 2.4 Statistická data o kybernetické kriminalitě na území ČR

Na základě žádosti o poskytnutí statistických dat o kybernetické kriminalitě dle jednotlivých druhů a rovněž dle příslušných ustanovení trestního zákoníku, a to v rozsahu počet zjištěných skutků, počet objasněných skutků, výše vzniklé škody a výše zajištěných výnosů dle 106/1999 Sb. Zákona o svobodném přístupu k informacím odeslanou na Policejní prezidium ČR, byla autorovi diplomové práce tato data poskytnuta za období 1. 1. 2011 až 31. 12. 2018 s výjimkou dat o výši zajištěných výnosů, kterou Policie ČR nevykazuje. Trestné činy jsou v statistice rozděleny na „objasněné“ a „neobjasněné“. Škody jsou v letech 2011 – 2015 uváděny ve stovkách Kč a v období 2016 – 2018 jsou uváděny v přesných hodnotách na jednotky Kč. [40]

# 3 CÍL PRÁCE A HYPOTÉZY

## 3.1 Stanovení cíle práce

Obecným cílem práce bylo zpracování problematiky kybernetické kriminality a analýza statistických dat kybernetické kriminality, která byla zaznamenána na území České republiky v období 2011-2018. Na základě tohoto obecného cíle byla práce koncipována do teoretické a do praktické části, kdy každá z těchto částí měla vlastní cíl.

Cílem teoretické části bylo čtenáři přiblížit problematiku kybernetické kriminality, její technické specifikace, jednotlivé druhy a základní legislativní úpravu.

Praktická část práce byla zaměřena na statistickou analýzu dat o kybernetické kriminalitě na území České republiky v období 2011-2018, která poskytlo Policejní prezidium České republiky, a prognózu vývoje na další období 3 let. Analytická část se skládá z grafů a tabulek, kde jsou uvedeny popisné statistiky a popisovány elementární charakteristiky časové řady indexu kybernetické kriminality. Tato data byla popisována ve dvou částech. První část analýzy se zaměřila na celkové počty spáchaných trestných činů a jejich rozdělení dle příslušných hlav trestního zákoníku, které daná trestná činnost porušuje. Druhá část této analýzy se zaměřila na data o způsobených finančních škodách kybernetickou kriminalitou v celkovém součtu a rozdělení do skupin dle výše způsobených škod. Prognóza na další období 3 let je vyjádřena pomocí grafů a tabulek, za použití trendových funkcí při předpokladu stejného počtu obyvatelstva České republiky. V závěru praktické části jsme se pokusili odhadnout dopady kybernetické kriminality na obyvatelstvo České republiky a vytvořit souhrnné doporučení, jak se kriminalitě tohoto druhu co nejefektivněji bránit.

## 3.2 Stanovené hypotézy

**Hypotéza č. 1:**

*„Předpokládá se, že ekonomicky orientovaná registrovaná kybernetická kriminalita tvoří více než 50 % z celkového počtu trestných činů v rámci kybernetické kriminality.“*

**Hypotéza č. 2:**

*„Předpokládá se, že meziroční nárůst registrované kybernetické kriminality činí průměrně více než 20 %.“*

**Hypotéza č. 3:**

*„Předpokládá se, že prognóza registrované kybernetické kriminality na další 3 roky předpoví, že se počet trestných činů zvýší o více než 500 % oproti začátku sledovaného období“*

**Hypotéza č. 4:**

*„Předpokládá se, že prognóza registrované kybernetické kriminality na další 3 roky předpoví, že se způsobené finanční škody zvýší nad hranici 1 mld. Kč ročně.“*

# 4 METODIKA

V teoretické části byly vysvětleny jednotlivé druhy kybernetické kriminality, způsob jejich provedení, technické specifikace a pojmy nezbytné k pochopení principu kybernetické kriminality. Dále bylo vysvětleno postavení bezpečnostních složek v oblasti kybernetické kriminality na národní a mezinárodní úrovni.

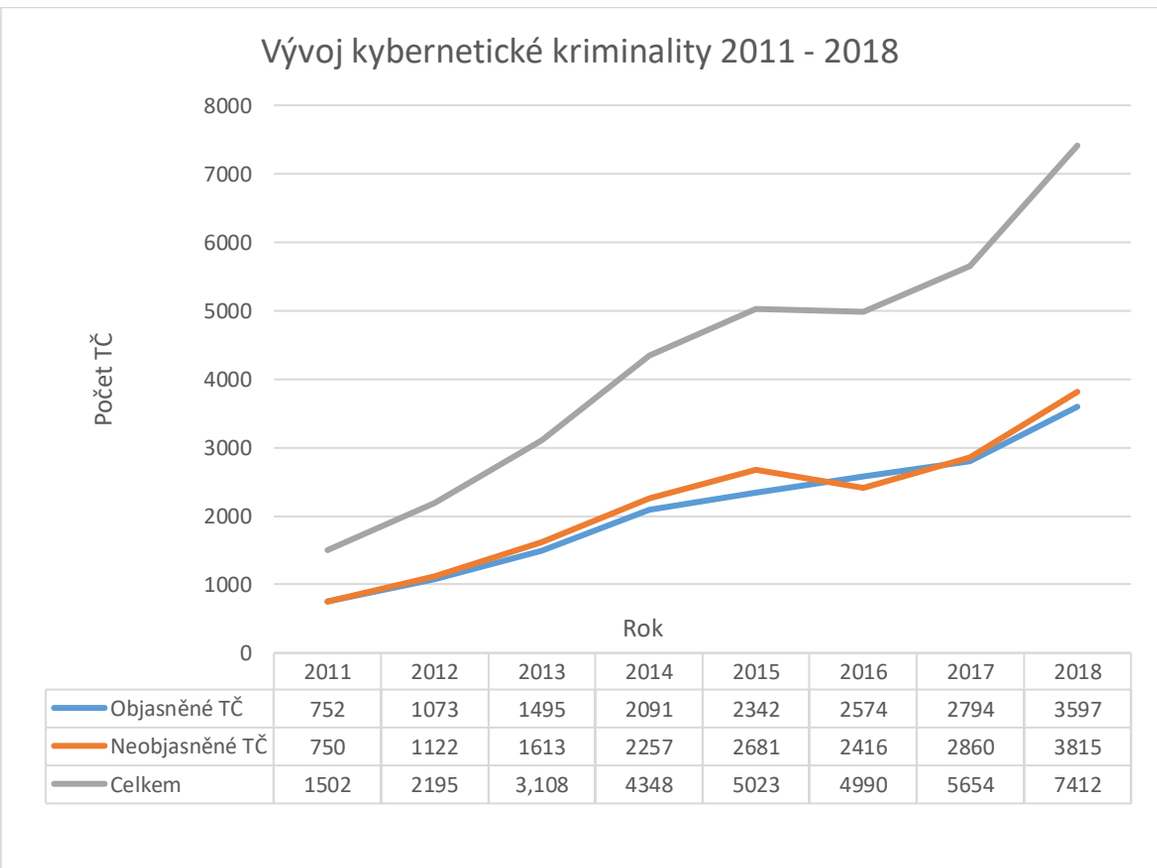
V praktické části budou uvedeny základní popisné statistiky evidované kybernetické kriminality na území České republiky za období 2011 - 2018. Pomocí analýzy a statistických metod bude provedeno vyhodnocení elementárních charakteristik časových řad registrované kybernetické kriminality na území České republiky. V rámci toho budeme taktéž využívat abdukci – vysvětlení pro pozorované jevy. Dále budou vyhodnoceny pomocí indukce dopady kybernetické kriminality na obyvatelstvo České republiky a pomocí trendových funkcí bude predikován předpokládaný vývoj této kriminality na období následujících 3 let.

Časové řady jsou věcně a prostorově srovnatelná pozorování dat, která jsou jednoznačně uspořádána z hlediska času ve směru z minulosti do přítomnosti. Elementární charakteristiky časové řady pak popisují index přepočtu kybernetické kriminality na 100 000 obyvatel ($y_i$), první a druhou absolutní diferenci ($d_{1i}$, $d_{2i}$), koeficient růstu ($k_i$), relativní přírůstek ($r_i$) a bazický index ($y_i/y_0$).

# 5 VÝSLEDKY

## 5.1 Analýza dat o kybernetické kriminalitě dle počtu TČ

V grafu 1 je znázorněn vývoj trestné činnosti v oblasti kybernetické kriminality za období v letech 2011 - 2018 a rozdělení na trestné činy, které byly objasněny a neobjasněny. Je zřejmé, že mimo roky 2011 a 2016 bylo vždy více trestných činů neobjasněných, avšak i přes to je poměr vyrovnaný. Procentuálně byl největší rozdíl v roce 2015, kdy bylo neobjasněno 53,4 % trestné činnosti, oproti tomu v roce 2016 bylo objasněno nejvíce trestné činnosti v oblasti kybernetické kriminality a to 51,5 %.




| | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|---|---|
| Objasněné TČ | 752 | 1073 | 1495 | 2091 | 2342 | 2574 | 2794 | 3597 |
| Neobjasněné TČ | 750 | 1122 | 1613 | 2257 | 2681 | 2416 | 2860 | 3815 |
| Celkem | 1502 | 2195 | 3,108 | 4348 | 5023 | 4990 | 5654 | 7412 |

*Graf 1 Vývoj kybernetické kriminality 2011-2018 [40]*

V popisu časové řady indexu registrované trestné činnosti dosáhla první absolutní diference maxima v roce 2018, kdy dosahovala hodnoty 16,21, což značí zvýšení indexu trestné činnosti oproti roku 2017 o 30 %. Druhá absolutní diference dosáhla nejvyšší hodnoty v roce 2018, a došlo tak k nárůstu meziročního přírůstku o 263 %. Největší negativní hodnota byla v roce 2016 a to -6,74. Tím došlo ke snížení meziročního přírůstku kybernetické trestné činnosti o 106 % oproti předchozímu roku. V témže roce došlo také jako v jediném k poklesu celkové trestné činnosti, kdy hodnota koeficientu růstu byla 0,9913 a procentuálně tak klesl na necelých 99 % oproti předchozímu roku. Průměrný koeficient růstu za sledované období činil 26 %. Relativní přírůstek dosáhl svého maxima v roce 2012, kdy došlo k nárůstu oproti roku 2011 o 46 %. Bazický index v roce 2018 činil 4,8638 oproti začátku sledovaného období a celkově tak trestná činnost narostla na 486 % hodnoty roku 2011.

*Tabulka 1 Elementární charakteristiky časové řady indexu registrované TČ [40]*

| Rok | $y_i$ | $d_{1i}$ | $d_{2i}$ | $k_i$ | $r_i$ | $y_i / y_0$ |
|---|---|---|---|---|---|---|
| 2011 | 14,31 | - | - | - | - | - |
| 2012 | 20,89 | 6,58 | - | 1,4596 | 0,4596 | 1,4596 |
| 2013 | 29,57 | 8,68 | 2,11 | 1,4158 | 0,4158 | 2,0665 |
| 2014 | 41,31 | 11,74 | 3,06 | 1,3971 | 0,3971 | 2,8871 |
| 2015 | 47,64 | 6,33 | -5,41 | 1,1533 | 0,1533 | 3,3295 |
| 2016 | 47,23 | -0,41 | -6,74 | 0,9913 | -0,0087 | 3,3007 |
| 2017 | 53,39 | 6,16 | 6,58 | 1,1305 | 0,1305 | 3,7313 |
| 2018 | 69,60 | 16,21 | 10,04 | 1,3035 | 0,3035 | 4,8638 |
| Celkem | 323,94 | 55,29 | - | 1,2644 | x | x |

Následující tabulka rozděluje trestnou činnost do kategorií dle hlav trestního zákoníku, jejichž paragraf trestný čin porušuje. V kolonce „Obyvatelstvo“ je pak uveden počet obyvatel ČR v daný rok. Je zřejmé, že majoritní podíl zaujímají trestné činy porušující paragrafy hlavy V trestního zákoníku, což jsou trestné činy proti majetku. S počtem 23 999 trestných činů činí podíl z celkové trestné činnosti 70 % za sledované období. Druhou nejpočetnější kategorií jsou trestné činy hospodářské, zařazené pod hlavou VI trestního zákoníku s 10,5 %. Ekonomicky orientovaná trestná činnost tak činí 80 % z celkového počtu kybernetické kriminality. Nejpočetnější skupinou trestných činů, které neřadíme mezi ekonomickou trestnou činnost jsou prohřešky proti hlavě III trestního zákoníku, tedy trestné činy proti lidské důstojnosti v sexuální oblasti. S 2 379 trestnými činy je podíl této trestné činnosti z celkového počtu 6,9 %. Vzhledem k nízkému počtu vstupních dat, a tedy i nízké relevanci, budou vynechány popisy elementárních charakteristik časové řady indexů trestné činnosti spadající pod hlavy I, VIII a IX trestního zákoníku.

*Tabulka 2 Počet TČ dle hlav TZK a počet obyvatelstva [40,41]*

| Rok | I | II | III | IV | V | VI | VII | VIII | IX | X | XIII | Obyvatelstvo |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2011 | 0 | 84 | 92 | 40 | 1 011 | 187 | 11 | 0 | 0 | 73 | 4 | 10 496 672 |
| 2012 | 2 | 133 | 120 | 40 | 1 488 | 302 | 5 | 4 | 1 | 96 | 4 | 10 509 286 |
| 2013 | 0 | 166 | 228 | 30 | 2 232 | 267 | 42 | 4 | 0 | 134 | 5 | 10 510 719 |
| 2014 | 18 | 201 | 240 | 74 | 3 239 | 378 | 15 | 0 | 0 | 178 | 5 | 10 524 783 |
| 2015 | 1 | 247 | 283 | 71 | 3 729 | 502 | 13 | 2 | 1 | 164 | 10 | 10 542 942 |
| 2016 | 1 | 274 | 265 | 71 | 3 709 | 459 | 15 | 1 | 0 | 187 | 8 | 10 565 284 |
| 2017 | 2 | 317 | 479 | 82 | 3 916 | 569 | 36 | 0 | 1 | 243 | 9 | 10 589 526 |
| 2018 | 6 | 421 | 672 | 145 | 4 675 | 917 | 31 | 1 | 6 | 524 | 14 | 10 649 800 |
| Celkem | 30 | 1 843 | 2 379 | 553 | 23 999 | 3 581 | 168 | 12 | 9 | 1 599 | 59 | x |

U registrovaných skutků porušující hlavu II trestního zákoníku byl průměrný koeficient růstu 26 %. Nevyšší byl koeficient růstu hned v druhém roce sledovaného období (2012) a to 158 % hodnoty předchozího roku. První absolutní diference hodnotou 0,96 ukazuje, že k největšímu, 36% nárustu počtu skutků oproti předchozímu roku došlo v roce 2018. Ve stejném roce byla také nejvyšší druhá absolutní diference, kdy došlo k navýšení přírůstku o 240 %. Nejvyšší zpomalení růstu pak bylo zaznamenáno v roce 2016, kdy přírůstek dosahoval 58 % hodnoty přírůstku předchozího roku. Bazický index ukázal nárůst v roce 2018 o 493 % oproti roku 2011 a je tak srovnatelný s bazickým indexem celkového počtu kybernetické kriminality.

*Tabulka 3 Elementární charakteristiky časové řady indexu registrované TČ hlavy II TZK [40]*

| Rok | $y_i$ | $d_{1i}$ | $d_{2i}$ | $k_i$ | $r_i$ | $y_i / y_0$ |
|---|---|---|---|---|---|---|
| 2011 | 0,80 | - | - | - | - | - |
| 2012 | 1,27 | 0,47 | - | 1,5814 | 0,5814 | 1,5814 |
| 2013 | 1,58 | 0,31 | -0,15 | 1,2480 | 0,2480 | 1,9735 |
| 2014 | 1,91 | 0,33 | 0,02 | 1,2092 | 0,2092 | 2,3865 |
| 2015 | 2,34 | 0,43 | 0,10 | 1,2267 | 0,2267 | 2,9276 |
| 2016 | 2,59 | 0,25 | -0,18 | 1,1070 | 0,1070 | 3,2407 |
| 2017 | 2,99 | 0,40 | 0,15 | 1,1543 | 0,1543 | 3,7407 |
| 2018 | 3,95 | 0,96 | 0,56 | 1,3206 | 0,3206 | 4,9398 |
| Celkem | 17,44 | 3,15 | - | 1,2639 | x | x |

U trestných činů proti lidské důstojnosti v sexuální oblasti je nejčastěji porušován § 192 - Výroba a jiné nakládání s dětskou pornografií. Tento paragraf byl za sledované období porušen celkem 1442x, což procentuálně činí 60,9 %. První absolutní diference v letech 2017 a 2018 zaznamenala skokové navýšení o hodnoty 2,02 a 1,79, tedy nárůst o 80 % a 39,5 %. Relativní přírůstek ovšem dosáhl nejvyšší hodnoty v roce 2013, kdy došlo k zvýšení registrované trestné činnosti o 90 %. Druhá absolutní diference ukazuje, že v roce 2014 došlo k největšímu poklesu meziročního přírůstku, který se snížil o 89 %. Průměrný koeficient růstu za sledované období činí 37 % a bazický index dosáhl 720 %. Trestné činy proti hlavě III trestního zákoníku jsou tak nejstrměji rostoucí registrovanou kybernetickou kriminalitou vůbec. Ani takový statistický nárůst ovšem nemusí znamenat celkové zvýšení kriminality tohoto druhu (zejména pak § 192), ale můžeme ho připisovat rozmachu informačních technologií ve sledovaném období a následnému přesunu této kriminality do virtuálního prostředí z fyzických médií (papír, DVD, apod.).

*Tabulka 4 Elementární charakteristiky časové řady indexu registrované TČ hlavy III TZK [40]*

| Rok | $y_i$ | $d_{1i}$ | $d_{2i}$ | $k_i$ | $r_i$ | $y_i / y_0$ |
|---|---|---|---|---|---|---|
| 2011 | 0,88 | - | - | - | - | - |
| 2012 | 1,14 | 0,27 | - | 1,3028 | 0,3028 | 1,3028 |
| 2013 | 2,17 | 1,03 | 0,76 | 1,8997 | 0,8997 | 2,4749 |
| 2014 | 2,28 | 0,11 | -0,92 | 1,0512 | 0,0512 | 2,6017 |
| 2015 | 2,68 | 0,40 | 0,29 | 1,1771 | 0,1771 | 3,0626 |
| 2016 | 2,51 | -0,18 | -0,58 | 0,9344 | -0,0656 | 2,8617 |
| 2017 | 4,52 | 2,02 | 2,19 | 1,8034 | 0,8034 | 5,1609 |
| 2018 | 6,31 | 1,79 | -0,23 | 1,3950 | 0,3950 | 7,1993 |
| Celkem | 22,49 | 5,43 | - | 1,3662 | x | x |

V rámci hlavy IV trestního zákoníku byly porušovány ve sledovaném období až na dvě výjimky pouze § 201 - Ohrožování mravní výchovy dítěte a § 202 - Svádění k pohlavnímu styku. § 201 se na celkovém počtu 553 registrovaných skutků podílí 64 %. V roce 2014 došlo k nejvyššímu procentuálnímu nárůstu, kdy při hodnotě první absolutní diference 0,42 nám koeficient růstu vykazoval nárůst o 146 procent. První absolutní diference dosáhla maxima při druhém skokovém nárůstu, který byl zaznamenán v roce 2018, a to hodnotou 0,59, což dle koeficientu růstu činilo 76 %. Druhá absolutní diference byla nejnižší v roce 2015, kdy se po nárůstu v předchozím roce počet registrovaných skutků mírně snížil, a dosahovala hodnoty -0,45, což činí pokles meziročního nárůstku o 107 %. Celkově byl největší pokles v roce 2013, kdy byl relativní přírůstek -25 % a průměrný koeficient růstu činil 30 %. Bazický index v roce 2018 dosahoval 357 %.

*Tabulka 5 Elementární charakteristiky časové řady indexu registrované TČ hlavy IV TZK [40]*

| Rok | $y_i$ | $d_{1i}$ | $d_{2i}$ | $k_i$ | $r_i$ | $y_i / y_0$ |
|---|---|---|---|---|---|---|
| 2011 | 0,38 | - | - | - | - | - |
| 2012 | 0,38 | 0,00 | - | 0,9988 | -0,0012 | 0,9988 |
| 2013 | 0,29 | -0,10 | -0,09 | 0,7499 | -0,2501 | 0,7490 |
| 2014 | 0,70 | 0,42 | 0,51 | 2,4634 | 1,4634 | 1,8451 |
| 2015 | 0,67 | -0,03 | -0,45 | 0,9578 | -0,0422 | 1,7672 |
| 2016 | 0,67 | 0,00 | 0,03 | 0,9979 | -0,0021 | 1,7635 |
| 2017 | 0,77 | 0,10 | 0,10 | 1,1523 | 0,1523 | 2,0320 |
| 2018 | 1,36 | 0,59 | 0,48 | 1,7583 | 0,7583 | 3,5729 |
| Celkem | 5,23 | 0,98 | - | 1,2969 | x | x |

Trestné činy proti majetku jsou jednoznačně nejčastějším druhem kybernetické kriminality. Nejvíce je porušován § 209 - Podvod. Za sledované období bylo evidováno 16072 skutků, což činí 67 % z trestné činnosti proti hlavě V a 47 % z celkové trestné činnosti. Můžeme se domnívat, že toto číslo je tak vysoké zejména díky různým formám phishingových útoků, které jsou jednoduše proveditelné i ve vysokém počtu. V rámci této trestné činnosti nám první absolutní diference dosáhla nejvyšších hodnot v roce 2014, a to 9,54, což bylo se 45 % třetí nejvyšším relativním přírůstkem. Ten byl nejvyšší v roce 2013 a dosahoval 50 %. Druhá absolutní diference měla negativní hodnoty dva roky po sobě, a to v roce 2015 a 2016. Hodnoty -4,96 a -4,89 vykazují pokles meziročního přírůstku o 52 % a 105 %, čímž se v roce 2016 lehce snížil celkový počet této trestné činnosti. Průměrný koeficient růstu byl ve sledovaném období 26 % a bazický index na konci sledovaného období byl 456 % původní hodnoty.

*Tabulka 6 Elementární charakteristiky časové řady indexu registrované TČ hlavy V TZK [40]*

| Rok | $y_i$ | $d_{1i}$ | $d_{2i}$ | $k_i$ | $r_i$ | $y_i / y_0$ |
|---|---|---|---|---|---|---|
| 2011 | 9,63 | - | - | - | - | - |
| 2012 | 14,16 | 4,53 | - | 1,4700 | 0,4700 | 1,4700 |
| 2013 | 21,24 | 7,08 | 2,55 | 1,4998 | 0,4998 | 2,2048 |
| 2014 | 30,77 | 9,54 | 2,46 | 1,4492 | 0,4492 | 3,1952 |
| 2015 | 35,37 | 4,59 | -4,94 | 1,1493 | 0,1493 | 3,6722 |
| 2016 | 35,11 | -0,26 | -4,86 | 0,9925 | -0,0075 | 3,6448 |
| 2017 | 36,98 | 1,87 | 2,14 | 1,0534 | 0,0534 | 3,8394 |
| 2018 | 43,90 | 6,92 | 5,04 | 1,1871 | 0,1871 | 4,5576 |
| Celkem | 227,15 | 34,27 | - | 1,2573 | x | x |

V rámci hospodářských trestných činů docházelo nejčastěji k porušování § 234 - Neoprávněné opatření, padělání a pozměnění platebního prostředku a § 270 - Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi. Poměrově pak byl § 234 porušen v 31 % případů hospodářské trestné činnosti v rámci kybernetické kriminality a § 270 dokonce v 63 %. Elementární charakteristiky časové řady nám v rámci první a druhé absolutní diference dosahují nejvyšších hodnot v roce 2018, kdy první absolutní diference s hodnotou 3,24 ukazuje nárůst indexu o 60 % a druhá absolutní diference s hodnotou 2,21 činí nárůst přírůstku meziročně na 214 % předchozího roku. Průměrný koeficient růstu činil 28 % a dle relativního přírůstku byl v také zaznamenán pokles této trestné činnosti, kdy celkový počet v roce 2013 klesl o 11,6 % a v roce 2016 o 8,7 %. Bazický index byl v roce 2018 srovnatelný s bazickým indexem celkové kybernetické kriminality a činil 483 %.

*Tabulka 7 Elementární charakteristiky časové řady indexu registrované TČ hlavy VI TZK [40]*

| Rok | $y_i$ | $d_{1i}$ | $d_{2i}$ | $k_i$ | $r_i$ | $y_i / y_0$ |
|---|---|---|---|---|---|---|
| 2011 | 1,78 | - | - | - | - | - |
| 2012 | 2,87 | 1,09 | - | 1,6130 | 0,6130 | 1,6130 |
| 2013 | 2,54 | -0,33 | -1,43 | 0,8840 | -0,1160 | 1,4259 |
| 2014 | 3,59 | 1,05 | 1,38 | 1,4138 | 0,4138 | 2,0160 |
| 2015 | 4,76 | 1,17 | 0,12 | 1,3258 | 0,3258 | 2,6727 |
| 2016 | 4,34 | -0,42 | -1,59 | 0,9124 | -0,0876 | 2,4386 |
| 2017 | 5,37 | 1,03 | 1,45 | 1,2368 | 0,2368 | 3,0161 |
| 2018 | 8,61 | 3,24 | 2,21 | 1,6025 | 0,6025 | 4,8332 |
| Celkem | 33,88 | 6,83 | - | 1,2840 | x | x |

Hlava VIII trestního zákoníku popisuje trestné činy obecně nebezpečné a mezi porušované paragrafy v této skupině patří hlavně § 279 - Nedovolené ozbrojování s 21 %, § 287 - Šíření toxikomanie s 27 % a nejvíce se jednalo o § 283 - Nedovolená výroba a jiné nakládání s omamnými a psychotropními látkami a s jedy s 38 % z evidované trestné činnosti. V rámci kybernetické kriminality byla tato trestná činnost evidována v rámci desítek trestných činů ročně. V roce 2013 došlo k vysokému nárůstu, kdy relativní přírůstek činil 739 %, ovšem v roce následujícím došlo k jeho poklesu o 64 %. Průměrný koeficient růstu za sledované období činí 106 %. Ten je hodně ovlivněn právě rokem 2013, kdy dosahoval maxima i bazický index a to 381 %. V roce 2018 bazický index činil 278 %.

*Tabulka 8 Elementární charakteristiky časové řady indexu registrované TČ hlavy VII TZK [40]*

| Rok | $y_i$ | $d_{1i}$ | $d_{2i}$ | $k_i$ | $r_i$ | $y_i / y_0$ |
|---|---|---|---|---|---|---|
| 2011 | 0,10 | - | - | - | - | - |
| 2012 | 0,05 | -0,06 | - | 0,4540 | -0,5460 | 0,4540 |
| 2013 | 0,40 | 0,35 | 0,41 | 8,3989 | 7,3989 | 3,8131 |
| 2014 | 0,14 | -0,26 | -0,61 | 0,3567 | -0,6433 | 1,3600 |
| 2015 | 0,12 | -0,02 | 0,24 | 0,8652 | -0,1348 | 1,1766 |
| 2016 | 0,14 | 0,02 | 0,04 | 1,1514 | 0,1514 | 1,3548 |
| 2017 | 0,34 | 0,20 | 0,18 | 2,3945 | 1,3945 | 3,2440 |
| 2018 | 0,29 | -0,05 | -0,25 | 0,8562 | -0,1438 | 2,7777 |
| Celkem | 1,59 | 0,19 | - | 2,0681 | x | x |

U hlavy X trestního zákoníku docházelo ve sledovaném období nejčastěji k porušování § 353 - Nebezpečné vyhrožování, kdy podíl těchto skutků byl 37 % a § 354 - Nebezpečné pronásledování s podílem 29 %. Tyto dva trestné činy spolu úzce souvisejí a mohou se vzájemně prolínat. V rámci kybernetické kriminality je pak dáváme do souvislosti se cyberstalkingem, zejména pak § 354, a také se zmíněným rozmachem informačních technologií, které jsou součástí každodenního života a kvůli jejich dostupnosti je nesmírně jednoduché je zneužívat v rámci trestné činnosti tohoto druhu. Z tabulky je zřejmé, že k nejvyššímu nárůstu trestných činů v rámci hlavy X došlo v roce 2018, kdy první absolutní diference dosáhla hodnoty 2,63 a koeficient růstu tak ukázal navýšení o 114 %. Nejvyšší nárůst byl i v rámci druhé absolutní diference. S hodnotou 2,10 došlo ke vzrůstu meziročního přírůstku o 396 % oproti předchozímu roku. Průměrný koeficient růstu byl ve sledovaném období 36 % a bazický index v roce 2018 dosáhl hodnoty 708 %, který je výrazně nad celkovým bazickým indexem. Takový nárůst může být vysvětlen tím, že se bezpečnostní složky začaly více zajímat o prostředí sociálních sítí a negativních projevů chování jejich uživatelů.

*Tabulka 9 Elementární charakteristiky časové řady indexu registrované TČ hlavy X TZK [40]*

| Rok | $y_i$ | $d_{1i}$ | $d_{2i}$ | $k_i$ | $r_i$ | $y_i / y_0$ |
|---|---|---|---|---|---|---|
| 2011 | 0,70 | - | - | - | - | - |
| 2012 | 0,91 | 0,22 | - | 1,3135 | 0,3135 | 1,3135 |
| 2013 | 1,27 | 0,36 | 0,14 | 1,3956 | 0,3956 | 1,8332 |
| 2014 | 1,69 | 0,42 | 0,05 | 1,3266 | 0,3266 | 2,4318 |
| 2015 | 1,56 | -0,14 | -0,55 | 0,9198 | -0,0802 | 2,2367 |
| 2016 | 1,77 | 0,21 | 0,35 | 1,1378 | 0,1378 | 2,5450 |
| 2017 | 2,29 | 0,52 | 0,31 | 1,2965 | 0,2965 | 3,2996 |
| 2018 | 4,92 | 2,63 | 2,10 | 2,1442 | 1,1442 | 7,0749 |
| Celkem | 15,12 | 4,22 | - | 1,3620 | x | x |

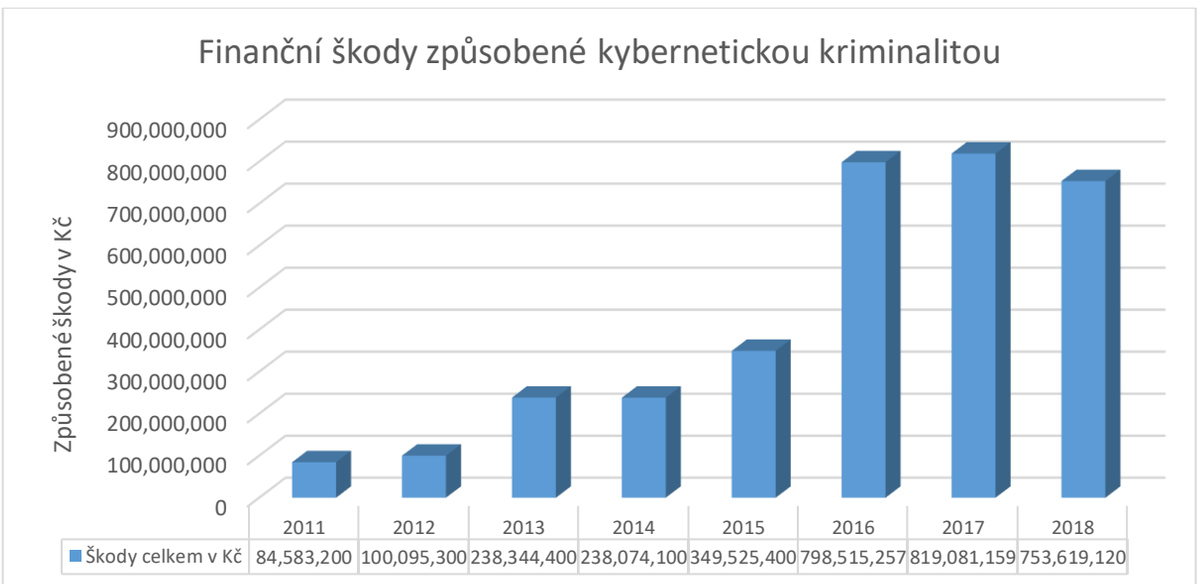
Jako poslední budou popsány trestné činy spadající pod hlavu XIII trestního zákoníku, kde jsou uvedeny trestné činy proti lidskosti, míru a válečné trestné činy. Paragrafy porušované v této kategorii byly § 403 - Založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka, § 404 - Projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka a § 405 - Popírání, zpochybňování, schvalování a ospravedlňování genocidia. Tyto trestné činy byly evidovány v řádu jednotek ročně. Z celkového počtu byl největší podíl trestných činů proti § 404, a to 53 %, § 405 byl porušen v 29 % případů a § 403 v 18 %. První absolutní diference měla nejvyšší hodnoty v letech 2015 a 2018. Procentuálně pak činil nárůst v těchto letech dle koeficientu růstu v roce 2015 99 % a v roce 2018 54 %. Průměrně koeficient růstu činil 24 %. Relativní přírůstek vykazoval lehce negativní hodnoty v letech 2012 a 2014, kdy počet těchto trestných činů stagnoval a v roce 2016 byl zaznamenán pokles relativního přírůstku o 20 %. Bazický index byl v roce 2018 oproti roku 2011 na 345 %, a je tedy nižší než bazický index celkové kybernetické kriminality.

*Tabulka 10 Elementární charakteristiky časové řady indexu registrované TČ hlavy XIII TZK [40]*

| Rok | $y_i$ | $d_{1i}$ | $d_{2i}$ | $k_i$ | $r_i$ | $y_i / y_0$ |
|---|---|---|---|---|---|---|
| 2011 | 0,04 | - | - | - | - | - |
| 2012 | 0,04 | 0,00 | - | 0,9988 | -0,0012 | 0,9988 |
| 2013 | 0,05 | 0,01 | 0,01 | 1,2498 | 0,2498 | 1,2483 |
| 2014 | 0,05 | 0,00 | -0,01 | 0,9987 | -0,0013 | 1,2467 |
| 2015 | 0,09 | 0,05 | 0,05 | 1,9966 | 0,9966 | 2,4890 |
| 2016 | 0,08 | -0,02 | -0,07 | 0,7983 | -0,2017 | 1,9870 |
| 2017 | 0,08 | 0,01 | 0,03 | 1,1224 | 0,1224 | 2,2303 |
| 2018 | 0,13 | 0,05 | 0,04 | 1,5468 | 0,5468 | 3,4497 |
| Celkem | 0,56 | 0,09 | - | 1,2445 | x | x |

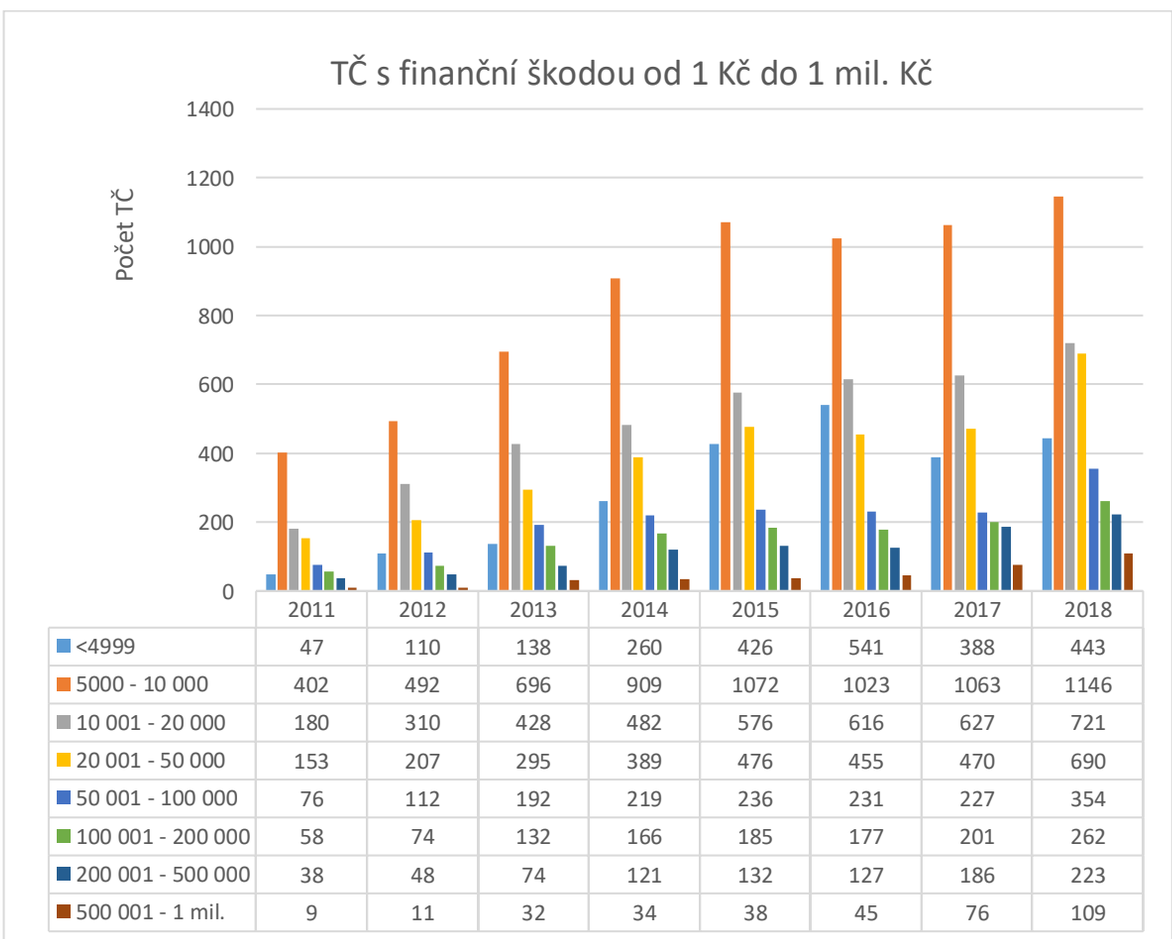
## 5.2 Analýza dat o kybernetické kriminalitě dle způsobených škod

V grafu finančních škod způsobených kybernetickou kriminalitou jsou uvedeny celkové finanční škody za každý rok ve sledovaném období na území ČR. Nejnižší byly škody způsobené v roce 2011 a to 84 583 200 Kč. Nejvíce škod bylo způsobeno v roce 2017, kdy se částka vyšplhala na 819 081 159 Kč a v následujícím roce mírně klesla na 753 619 120 Kč. Skokové nárůsty o více než násobek částky předchozího roku proběhly v roce 2013 z 100 095 300 Kč na 238 344 400 a v roce 2016 z 349 525 400 Kč na 798 515 257 Kč.




*Graf 2 Finanční škody způsobené kybernetickou kriminalitou [40]*

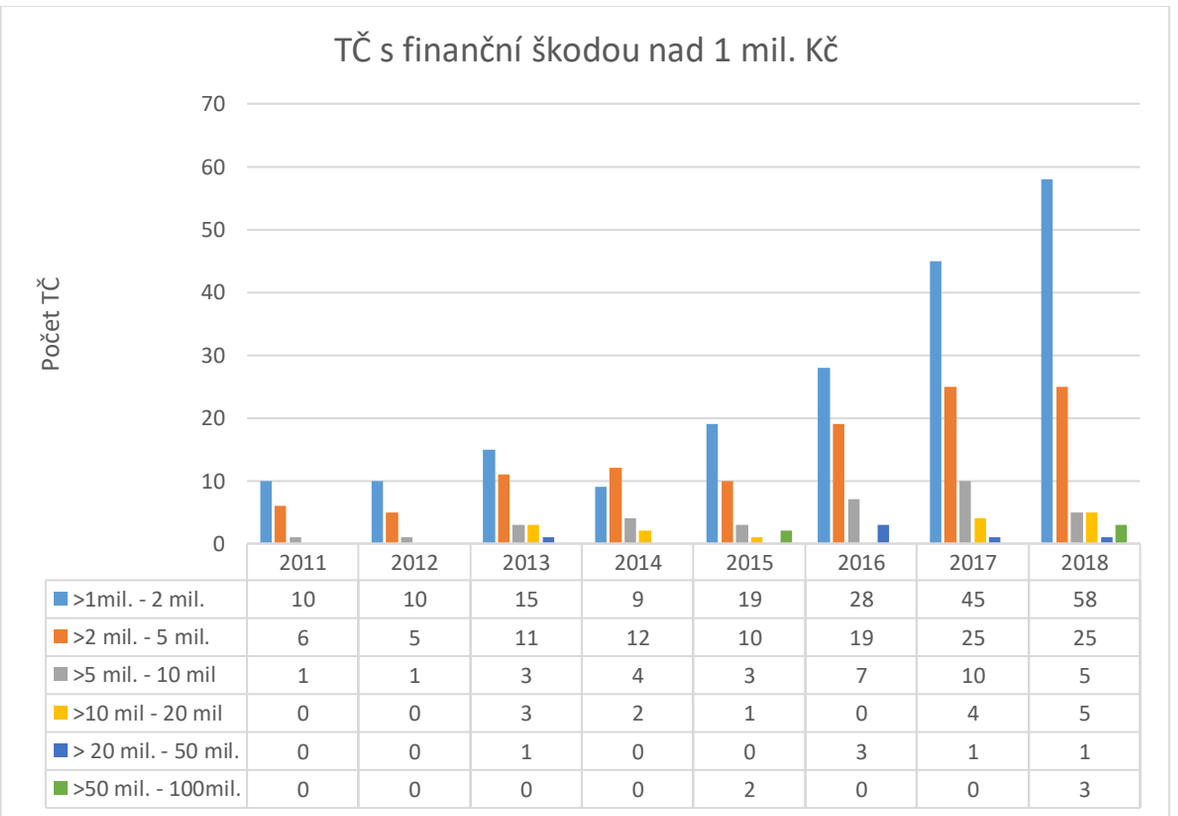
Při rozdělení finančních škod do kategorií zobrazených v grafu 3 je vidět, že nejvíce evidovaných skutků je ve skupině od 5000 Kč do 10 000 Kč, a to v celém sledovaném období. Počet trestných činů v této kategorii konstantně rostl až na rok 2016, kdy došlo k celkovému mírnému snížení kybernetické kriminality. Svého maxima pak dosáhly trestné činy v tomto rozsahu škod v roce 2018, a to 1146 trestných činů. Nejstrmější nárůst je zřejmý v kategorii škod do 4999 Kč, kdy v roce bylo takových skutků registrováno 47 a svého maxima dosáhla v roce 2016 s 541 registrovanými skutky. Dále kvantita trestné činnosti klesá s výší způsobených škod, ale až na pár výjimek, zejména v roce 2016, souměrně roste s postupujícím časem.




| | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|---|---|
| <4999 | 47 | 110 | 138 | 260 | 426 | 541 | 388 | 443 |
| 5000 - 10 000 | 402 | 492 | 696 | 909 | 1072 | 1023 | 1063 | 1146 |
| 10 001 - 20 000 | 180 | 310 | 428 | 482 | 576 | 616 | 627 | 721 |
| 20 001 - 50 000 | 153 | 207 | 295 | 389 | 476 | 455 | 470 | 690 |
| 50 001 - 100 000 | 76 | 112 | 192 | 219 | 236 | 231 | 227 | 354 |
| 100 001 - 200 000 | 58 | 74 | 132 | 166 | 185 | 177 | 201 | 262 |
| 200 001 - 500 000 | 38 | 48 | 74 | 121 | 132 | 127 | 186 | 223 |
| 500 001 - 1 mil. | 9 | 11 | 32 | 34 | 38 | 45 | 76 | 109 |

*Graf 3 TČ s finanční škodou od 1 Kč do 1 mil. Kč [40]*

Graf 4 obsahuje kategorie, kde jsou zařazeny trestné činy způsobující škody od 1 mil. Kč až do 100 mil. Nejvíce bylo evidováno trestných činů se škodami v rozpětí od 1 do 2 mil Kč. V této kategorii počet trestných činů poměrně stagnoval od 9 do 15 registrovaných skutků, ovšem od roku 2015 je zřejmé, že škod v tomto finančním rozsahu značně přibývá. Pokles trestné činnosti nastává v kategoriích od škod vyšších než 5 mil. Kč, kdy jejich počet pouze v letech 2017 a 2018 překročil hranici 10 trestných činů. Trestných činů, které způsobily škody nad 50 mil. bylo evidováno 5, kdy jako nejvyšší škoda byla zaznamenána částka 86 152 000 Kč, a stalo se tak v roce 2018.




| | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|---|---|
| >1mil. - 2 mil. | 10 | 10 | 15 | 9 | 19 | 28 | 45 | 58 |
| >2 mil. - 5 mil. | 6 | 5 | 11 | 12 | 10 | 19 | 25 | 25 |
| >5 mil. - 10 mil | 1 | 1 | 3 | 4 | 3 | 7 | 10 | 5 |
| >10 mil - 20 mil | 0 | 0 | 3 | 2 | 1 | 0 | 4 | 5 |
| > 20 mil. - 50 mil. | 0 | 0 | 1 | 0 | 0 | 3 | 1 | 1 |
| >50 mil. - 100mil. | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 3 |

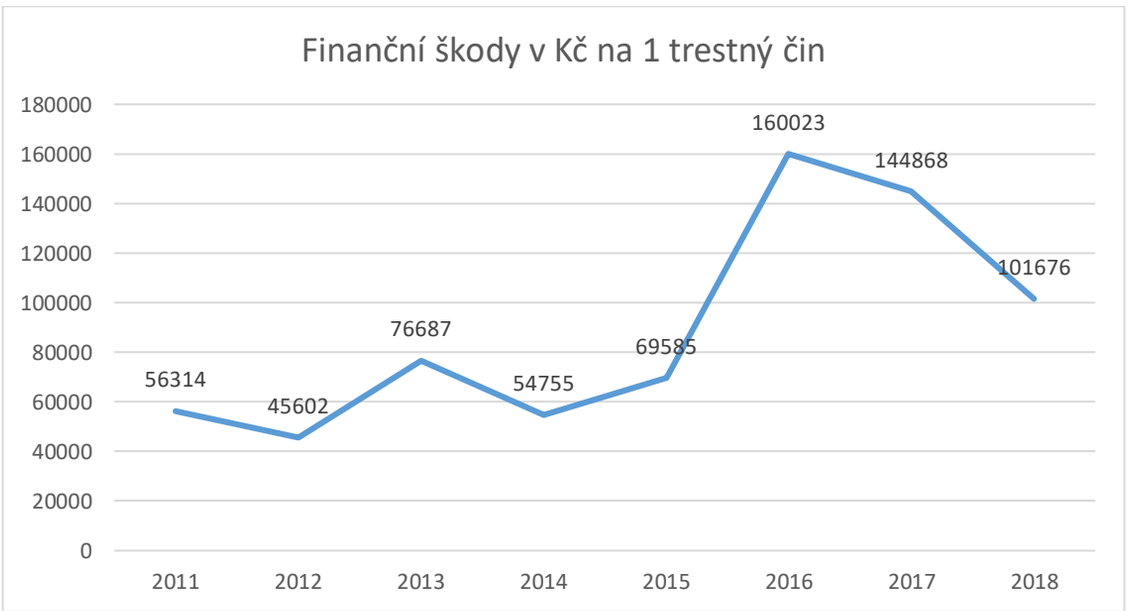
*Graf 4 TČ s finanční škodou nad 1 mil. Kč [40]*

V tabulce 11 jsou popsány elementární charakteristiky časové řady indexu způsobených škod kybernetickou kriminalitou. První absolutní diference dosáhla svého maxima v roce 2016, kdy došlo ke zvýšení o 4 242 660 oproti roku 2015 a koeficient růstu ukazuje procentuální navýšení o 128 %. Největší pokles byl v roce 2018, došlo tak snížení škod o 8 %. Druhá absolutní diference byla nejnižší v roce 2017, kdy se meziroční přírůstek snížil o 96 %. Maxima naopak dosáhla v roce 2016, kdy meziroční přírůstek vzrostl na 301 % hodnoty předchozího roku. Koeficient růstu dosahoval nejvyšší hodnoty v roce 2013, kdy došlo ke zvýšení škod o 138 % a průměrný koeficient růstu finančních škod byl ve sledovaném období 46 %. Bazický index byl nejvyšší v roce 2017, kdy dosáhl 960 % oproti roku 2011 a v roce 2018 klesl na 878 %. V porovnání s růstem bazického indexu počtu skutků, který činil v roce 2018 486 %, je bazický index škod téměř dvojnásobný. Tento jev můžeme dát do souvislosti se zvyšováním schopností zločinců v kybernetickém prostoru, kteří jsou schopni působit mnohem větší škody u páchané trestné činnosti.

*Tabulka 11 Elementární charakteristiky časové řady indexu škod registrované TČ [40]*

| Rok | $y_i$ | $d_{1i}$ | $d_{2i}$ | $k_i$ | $r_i$ | $y_i / y_0$ |
|---|---|---|---|---|---|---|
| 2011 | 805 809,69 | - | - | - | - | - |
| 2012 | 952 446,25 | 146 636,56 | - | 1,1820 | 0,1820 | 1,18 |
| 2013 | 2 267 631,74 | 1 315 185,49 | 1 168 548,94 | 2,3809 | 1,3809 | 2,81 |
| 2014 | 2 262 033,34 | -5 598,40 | -1 320 783,90 | 0,9975 | -0,0025 | 2,81 |
| 2015 | 3 315 254,89 | 1 053 221,55 | 1 058 819,95 | 1,4656 | 0,4656 | 4,11 |
| 2016 | 7 557 915,69 | 4 242 660,80 | 3 189 439,25 | 2,2797 | 1,2797 | 9,38 |
| 2017 | 7 734 823,63 | 176 907,94 | -4 065 752,86 | 1,0234 | 0,0234 | 9,60 |
| 2018 | 7 102 876,66 | -631 946,97 | -808 854,91 | 0,9183 | -0,0817 | 8,78 |
| Celkem | 31 998 791,87 | 6 297 066,97 | - | 1,4634 | x | x |

Graf 6 zobrazuje průměrné škody v přepočtu na jeden registrovaný trestný čin. V tomto grafu je zahrnuta veškerá registrovaná trestná činnost. Je zřejmé že v letech 2011 až 2015 průměrná výše škod kolísala, v roce 2016 došlo k strmému nárůstu o 129 % a v následujících letech opět klesala, a to v roce 2015 o 9,5 % a v roce 2018 dokonce o 30 %. Nárůst v roce 2016 je zapříčiněn skokovým zvýšením způsobených škod i přes mírné snížení počtu trestné činnosti v rámci kybernetické kriminality.



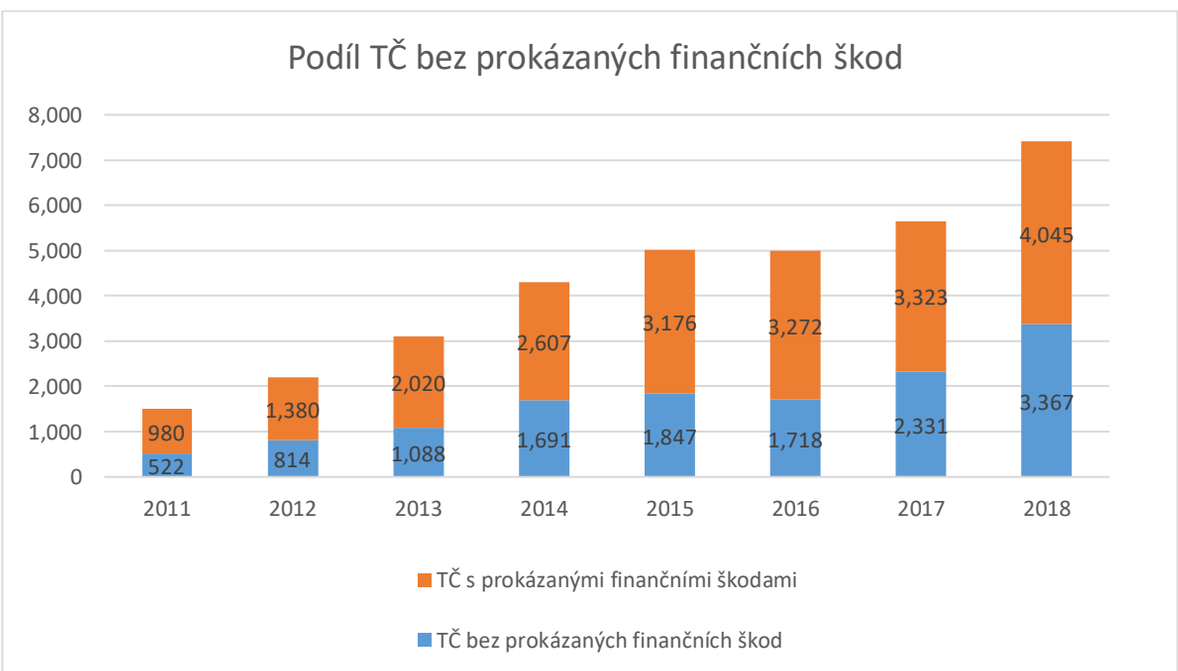

*Graf 5 Finanční škody v Kč na 1 trestný čin [40]*

V tabulce 12 jsou zobrazeny elementární charakteristiky časové řady indexu způsobených škod na jeden trestný čin z celkového počtu registrované kybernetické kriminality. Je zřejmé že vývoj průměrných škod nekoresponduje s vývojem počtu trestných činů a vykazuje kolísavé hodnoty. První absolutní diference měla největší nárůst v roce 2016, kdy hodnota 854,6 ukazuje zvýšení o 129 %. Naopak minimum bylo zaznamenáno v roce 2018 kdy s hodnotou -413,23 došlo k poklesu škod oproti roku 2017 o 30 %. V roce 2017 došlo taktéž k poklesu škod a to o 10 %. Koeficient přírůstku byl průměrně za sledované období na 19,5 %. Bazický index dosáhl svého maxima v roce 2016, kdy dosahoval hodnoty 282 % oproti začátku sledovaného období a v roce 2018 nakonec klesl na 178 %.

*Tabulka 12 Elementární charakteristiky časové řady indexu způsobených škod na jeden trestný čin [40]*

| Rok | $y_i$ | $d_{1i}$ | $d_{2i}$ | $k_i$ | $r_i$ | $y_i / y_0$ |
|---|---|---|---|---|---|---|
| 2011 | 536,49 | - | - | - | - | - |
| 2012 | 433,92 | -102,57 | - | 0,8088 | -0,1912 | 0,81 |
| 2013 | 729,61 | 295,69 | 398,27 | 1,6815 | 0,6815 | 1,36 |
| 2014 | 520,25 | -209,36 | -505,06 | 0,7130 | -0,2870 | 0,97 |
| 2015 | 660,01 | 139,77 | 349,13 | 1,2687 | 0,2687 | 1,23 |
| 2016 | 1514,61 | 854,60 | 714,83 | 2,2948 | 1,2948 | 2,82 |
| 2017 | 1368,03 | -146,59 | -1001,18 | 0,9032 | -0,0968 | 2,55 |
| 2018 | 954,72 | -413,31 | -266,72 | 0,6979 | -0,3021 | 1,78 |
| Celkem | 6717,64 | 418,23 | - | 1,1954 | x | x |

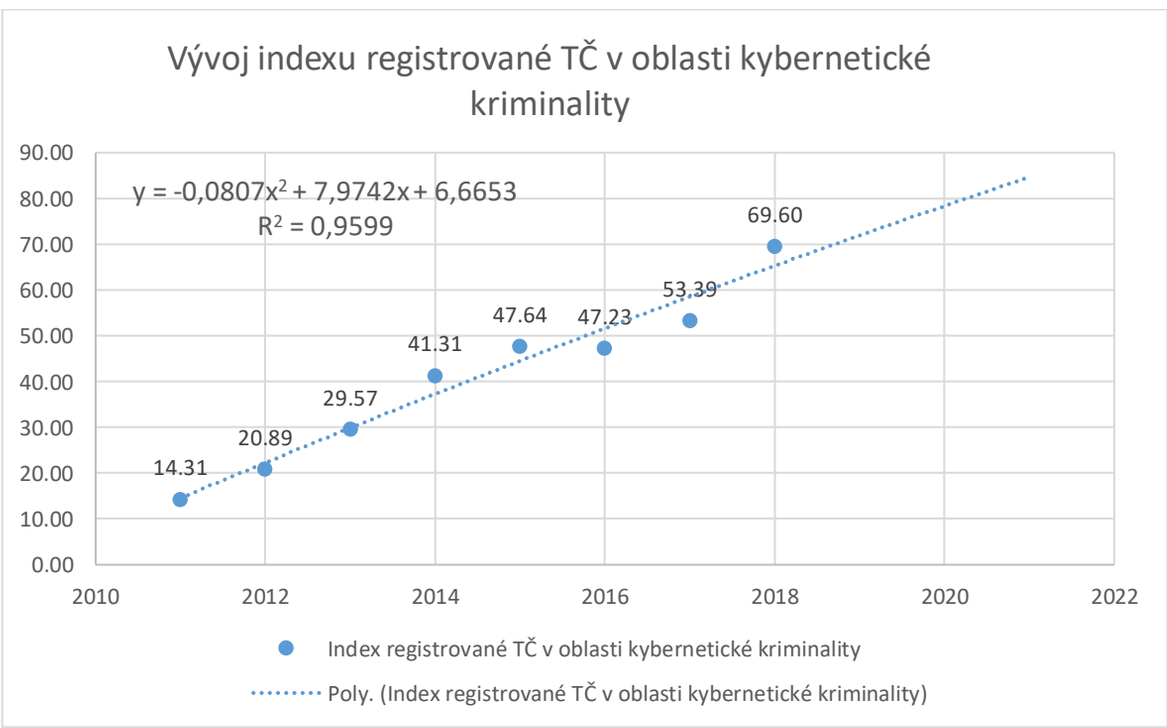
V grafu 6 je zobrazen podíl trestných činů s prokázanými finančními škodami a trestných činů bez prokázaných finančních škod. Procentuálně se podíl trestných činů bez prokázaných finančních škod pohyboval mezi 34 % až 45 %, kdy nejnižší podíl, tedy 34 %, byl v roce 2016, kdy došlo zároveň i k nejvyššímu meziročnímu nárůstu finančních škod, a nejvyšší 45 % v roce 2018, kdy se způsobené finanční škody naopak mírně snížily. 40% hranice dosahoval podíl trestných činů bez prokázaných finančních škod ještě jednou, a to v roce 2017, kdy tento podíl činil 41 %. V ostatních letech se podíl pohyboval mezi 34 % až 39 % a průměrně podíl trestných činů bez prokázaných finančních škod dosahoval ve sledovaném období 38 %.




*Graf 6 Podíl TČ bez prokázaných finančních škod [40]*

## 5.3 Prognóza kybernetické kriminality na další období

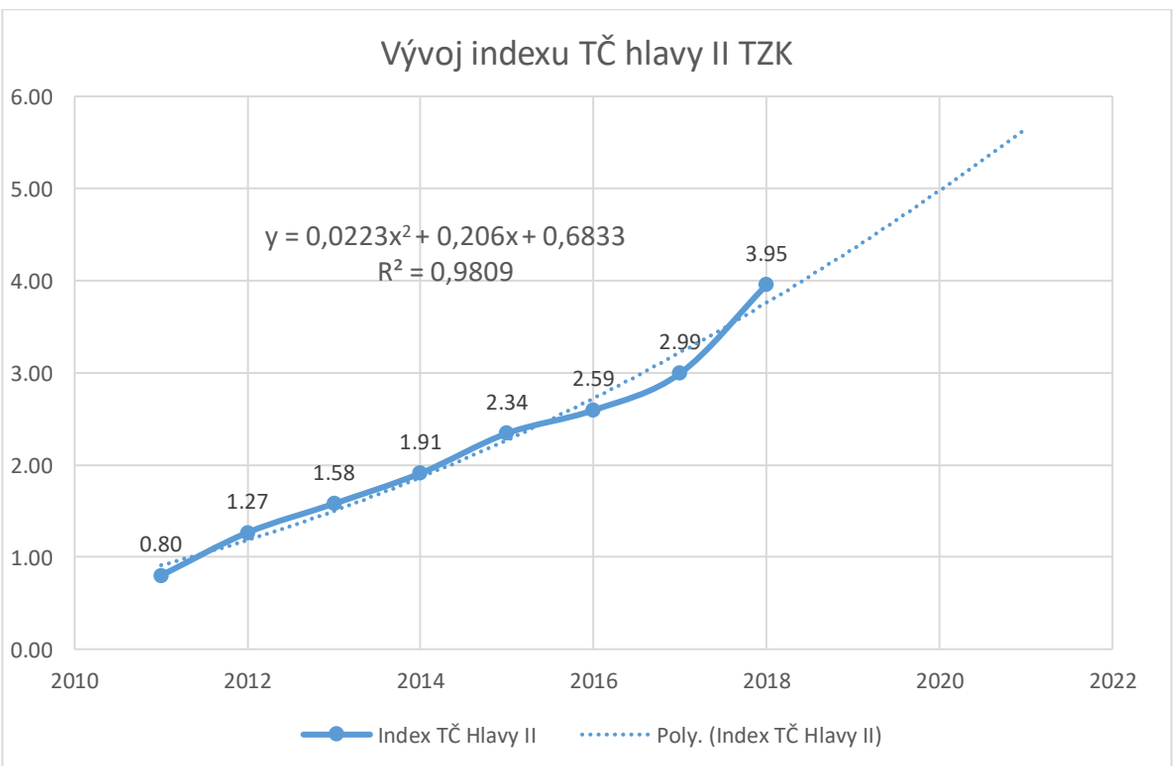
K prognóze na další období u indexu registrované trestné činnosti v oblasti kybernetické kriminality byla zvolena jako nejvhodnější polynomická trendová funkce ve tvaru rovnice $a + b*t_i + c*t_i^2$, kdy metodou nejmenších čtverců byly odhadnuty parametry rovnice jako „a = 6,653“, „b = 7,9742“ a „c = -0,0807“. Období na které předpovídáme vývoj trendu bylo určeno na následující 3 roky. Polynomická trendová funkce nám předpověděla hodnoty indexu registrované trestné činnosti pro rok 2019 „71,9“, 2020 „78,34“ a 2021 „84,62“. Index determinace k určení vhodnosti zvolené funkce byl vypočítán s hodnotou 0,9599 a index korelace 0,9794. V kombinaci s vypočítanou střední absolutní procentuální chybou odhadu, která činila 6 %, můžeme předpokládat, že tato prognóza je poměrně přesná. Průběh růstu dle polynomické trendové funkce by značil v období let 2019-2021 průměrný koeficient růstu 6,8 %, což je výrazně menší růst než ve sledovaném období, kdy tento průměr činil 26 %. Bazický index by se na konci předpovídaného období mohl vyšplhat na 591 % oproti roku 2011.




*Graf 7 Vývoj indexu registrované TČ v oblasti kybernetické kriminality [40]*

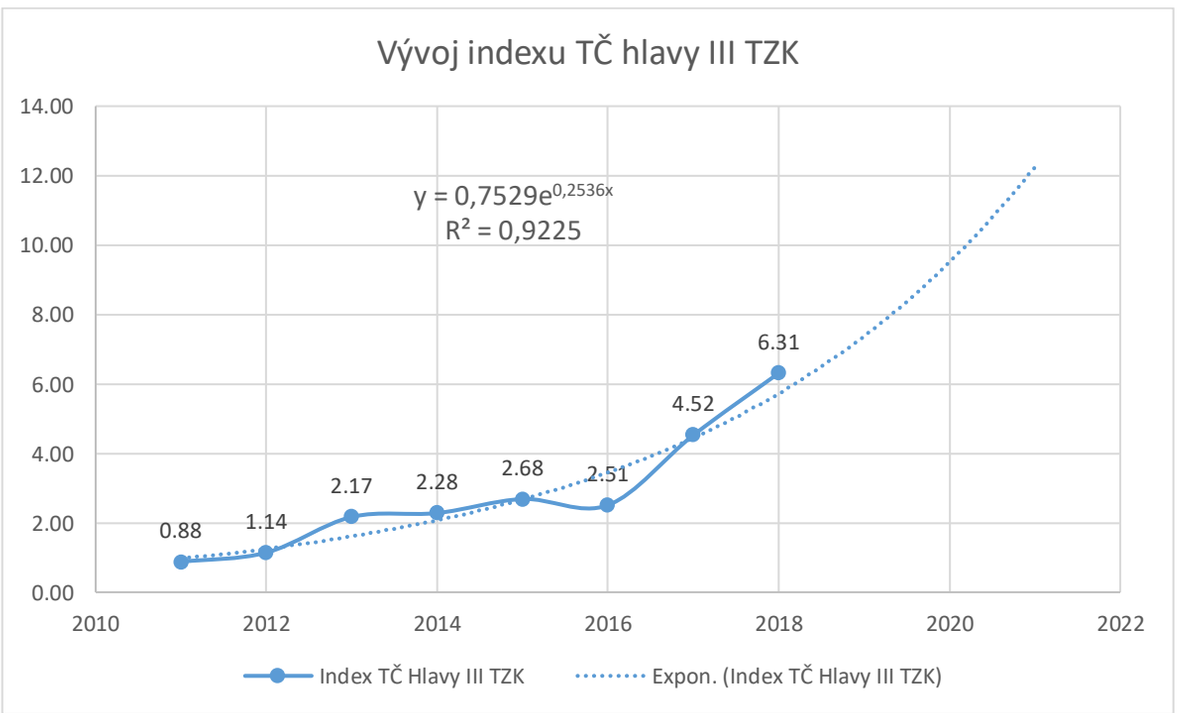
Prognóza vývoje indexu byla dále vypočítána také pro pět nejčastěji porušovaných hlav trestního zákoníku, což jsou jmenovitě hlavy II, III, V, VI a X.

Pro výpočet prognózy vývoje indexu v oblasti trestné činnosti proti hlavě II trestního zákoníku byla znovu zvolena jako nejvhodnější polynomická trendová funkce. Do rovnice polynomické trendové funkce ve tvaru $a + b*t_i + c*t_i^2$ byly odhadnuty parametry metodou nejmenších čtverců v následujících hodnotách „a = 0,6833“, „b = 0,206“ a „c = 0,0223“. Díky zvoleným parametrům nám vyšlo, že v roce 2019 se index trestné činnosti zvýší na hodnotu 4,34, v roce 2020 na 4,97 a v roce 2021 na 5,65. Index determinace v případě této funkce byl vypočten s hodnotou 0,9809, index korelace na 0,9845 a střední absolutní procentuální chyba dosáhla 5 %. Z těchto výpočtů můžeme určit, že tato prognóza na další tři roky vykazuje vysokou míru spolehlivosti a reálný vývoj tak může kopírovat předpovídaný trend.



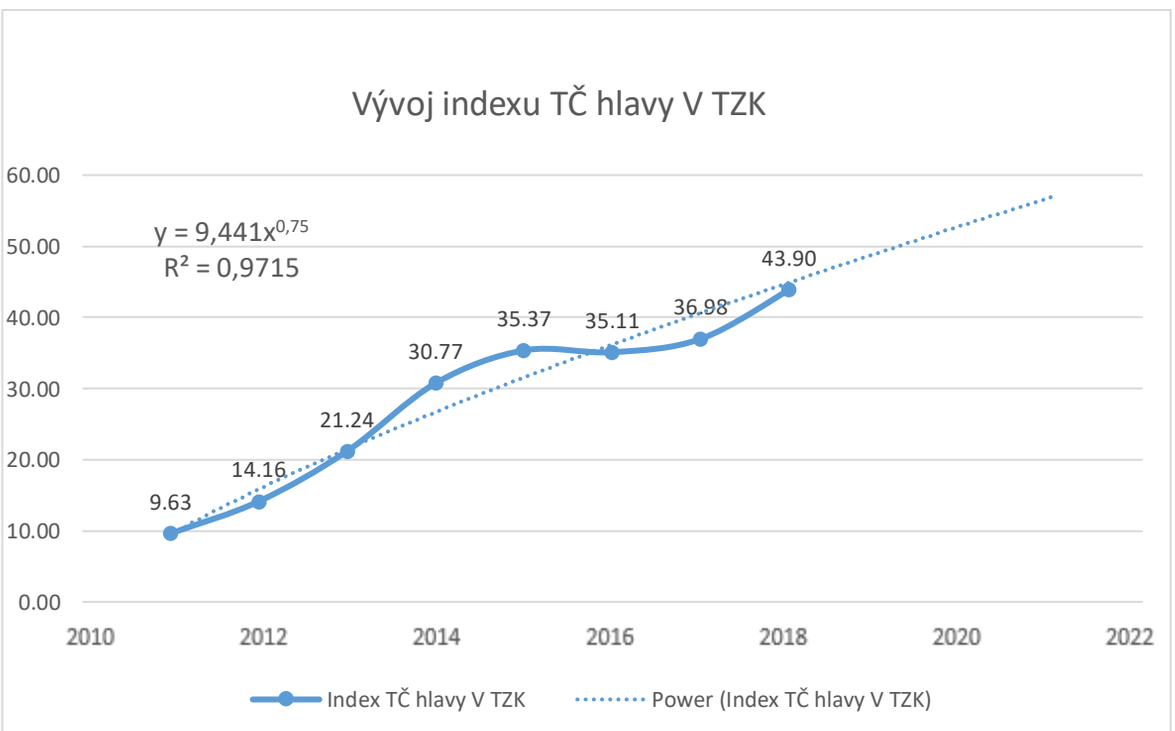

*Graf 8 Vývoj indexu TČ hlavy II TZK [40]*

V rámci stanovení prognózy pro index trestné činnosti v oblasti hlavy III trestního zákoníku byla stanovena jako nejvhodnější exponenciální trendová funkce. Do rovnice ve tvaru $y = a*e^{b*ti}$ byly metodou nejmenších čtverců odhadnuty dosazované hodnoty jako „a = 0,7529“ a „b = 0,2536“. Díky dosazení odhadnutých hodnot do rovnice byly vypočteny hodnoty pro následující období tak, že v roce 2019 dojde k zvýšení indexu na 7,38, v roce 2020 na 9,51 a v roce 2021 se by se index měl zvýšit až na hodnotu 12,25. Index determinace byl v rámci této trendové funkce vypočítán na 0,9225, index korelace na 0,9167 a střední absolutní procentuální chyba vykazuje hodnotu 20 %. V obraze vypočtených indexů pro vhodnost funkce se jedná o hrubý odhad možného vývoje této trestné činnosti v oblasti kybernetické kriminality. Je nutné ale také přihlédnout k charakteru trestné činnosti spadající pod hlavu III, kdy nelze vyloučit, že nová generace sexuálních násilníků, která bude jistě vykazovat mnohem větší zdatnost v oblasti IT než starší ročníky, nezapříčiní výrazný přesun nebo nárůst trestné činnosti tohoto charakteru v kybernetickém prostředí.



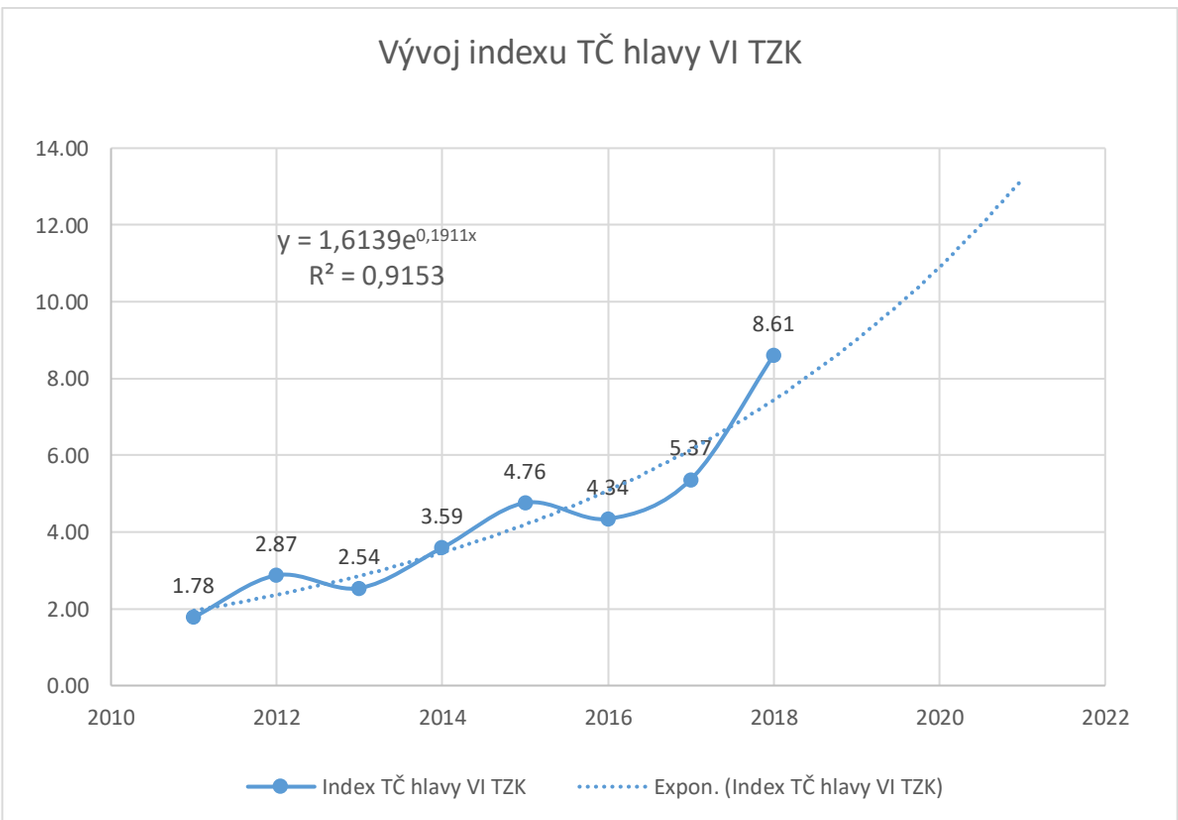

*Graf 9 Vývoj indexu TČ hlavy III TZK [40]*

Pro kategorii trestných činů proti hlavě V trestního zákoníku, která čítá největší podíl z celkového počtu kybernetické kriminality, byla zvolena pro stanovení prognózy vývoje indexu trestných činů mocninná trendová funkce. Pro rovnici mocninné trendové funkce ve tvaru „$y = a*t_i^b$“ byly odhadnuty hodnoty pomocí metody nejmenších čtverců následovně „a = 9,441“ a „b = 0,75“. Aplikací odhadnutých parametrů do rovnice byl předpovězen vývoj indexu pro rok 2019 na hodnotu 49,06, pro rok 2020 tento odhad činil 53,09 a pro poslední rok předpovídaného období tato hodnota vzrostla na 57,02. Vhodnost výběru funkce byla ověřena výpočtem indexu determinace s hodnotou 0,9715 a střední absolutní procentuální chybou dosahující 7 %. Index korelace činil 0,967. Zvolená trendová funkce tak ukazuje s poměrně vysokou mírou spolehlivosti možný vývoj pro nárůst trestné činnosti v rámci hlavy V. Je pravděpodobné, že majetková trestná činnost bude i nadále nejpočetněji zastoupenou trestnou činnosti v rámci kybernetické kriminality na území České republiky.



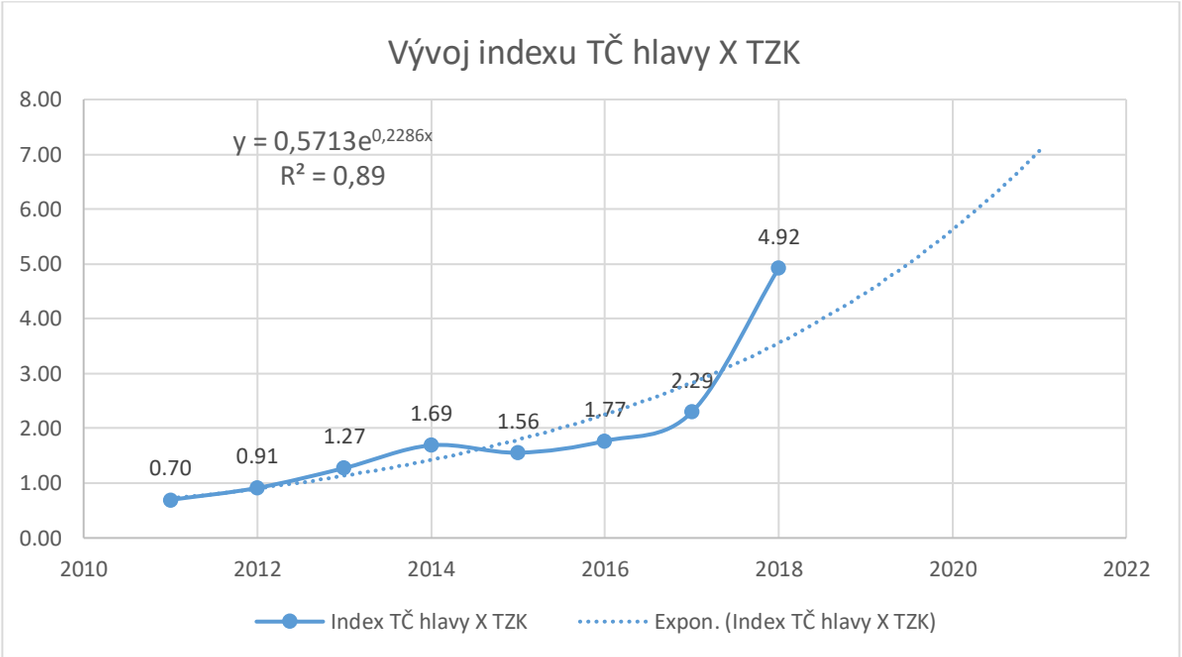

*Graf 10 Vývoj indexu TČ hlavy V TZK [40]*

U trestné činnosti v rámci hlavy VI trestního zákoníku byla k prognóze vývoje indexu trestné činnosti, která zvláště posledních dvou letech sledovaného období zaznamenala strmý nárůst, zvolena exponenciální trendová funkce. Pro stanovení budoucích hodnot indexu trestné činnosti, byly odhadnuty parametry rovnice pro výpočet ve tvaru $y = a*e^{b*ti}$ pomocí metody nejmenších čtverců, tak že hodnoty parametrů jsou „a = 1,6139“ a „b = 0,1911“. Po dosazení těchto odhadnutých parametrů do rovnice byly stanoveny hodnoty indexu na další období pro rok 2019 na 9,01, v roce 2020 by měl index činit 10,9 a v roce 2021 dokonce 13,21. Index determinace pro tuto zvolenou funkci byl vypočten na 0,9153 a střední procentuální chyba byla stanovena na 15 %. Index korelace dosahoval hodnoty 0,9148. Tato prognóza vykazuje nižší hodnoty důvěryhodnosti, avšak při bližším prozkoumání je vidět, že se v období 2016 - 2018 opakoval trend růstu z předchozích let. Za předpokladu, že se tato situace bude opakovat, mohou být hodnoty indexu v následujících letech podobné s předpovězeným průběhem.




*Graf 11 Vývoj indexu TČ hlavy VI TZK [40]*

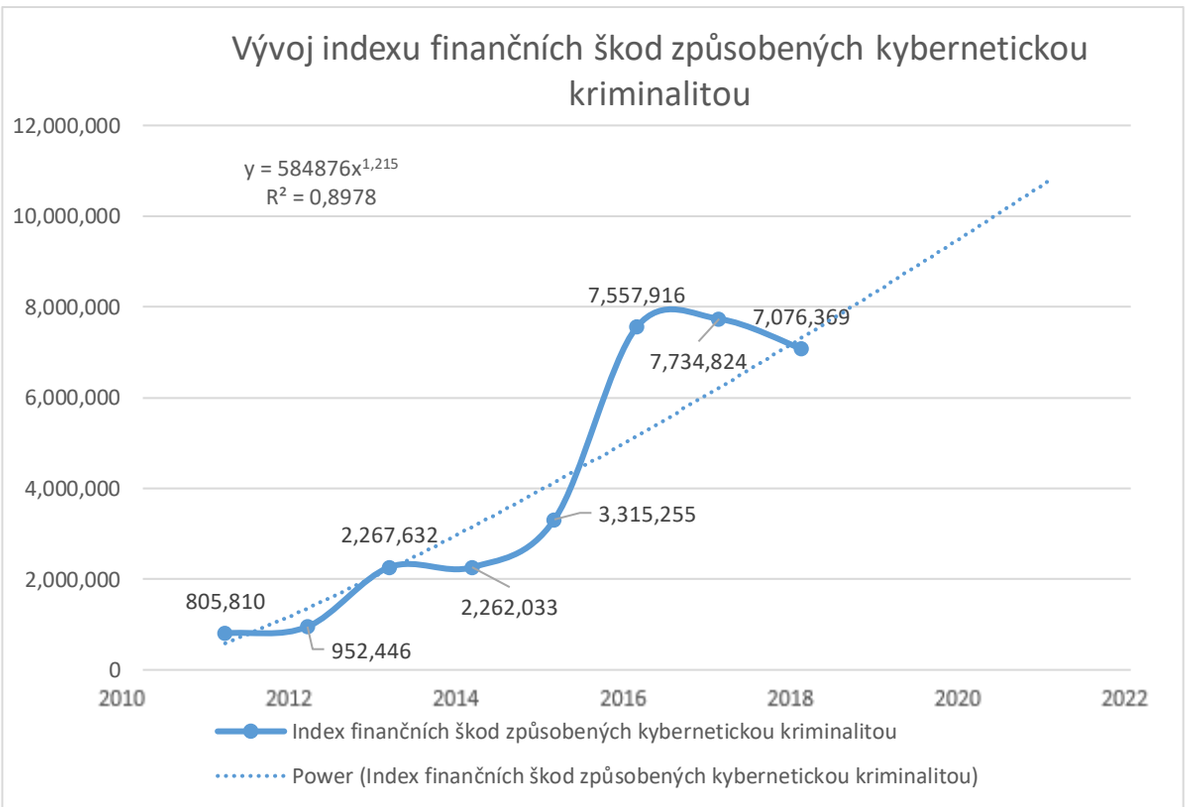
Stejně jako u předchozí kategorie byla pro prognózu vývoje indexu trestné činnosti v rámci hlavy X zvolena exponenciální funkce. Pro rovnici exponenciální funkce ve tvaru $y = a*e^{b*ti}$ byly pomocí metody nejmenších čtverců odhadnuty parametry funkce tak, že „a = 0,5713“ a „b = 0,2286“. Po dosazení odhadnutých parametrů do rovnice pro výpočet hodnot exponenciální trendové funkce, byly stanoveny předpokládané hodnoty vývoje indexu trestné činnosti pro rok 2019 na 4,47, pro rok 2020 činí hodnota indexu 5,6 a v roce by se dle předpokladu měl index vyšplhat na 7,06. Z indexu determinace, který činí 0,89, indexu korelace s hodnotou 0,83 a střední absolutní procentuální chyby, která dosahuje 26 % je zřejmé, že tento odhad je velice hrubý. Zvláště díky masivnímu nárůstu registrované trestné činnosti v roce 2018, tak i dle parametrů nejlépe hodnotící exponenciální funkce dosahuje nízké úrovně spolehlivosti. Lze předpokládat, že po takovém nárůstu může dojít ke zpomalení nárůstu nebo dokonce k poklesu, ale vzhledem k tomu, že porušovanými paragrafy jsou zejména § 353 a § 354 trestního zákoníku, můžeme předpokládat, že spíše než k masivnímu celkovému nárůstu tohoto druhu kriminality došlo buď k velkému přesunu do informačního prostředí, což je během jednoho roku nepravděpodobné, nebo PČR začala v tomto roce klasifikovat tuto trestnou činnost jinak než v letech předchozích, a došlo tak ovlivnění statistických dat. Tato varianta působí pravděpodobněji i s ohledem na fakt, že v roce 2018 nedošlo k žádnému většímu zpřístupnění technologií nebo komunikačních platforem, které by nebyly dostupné v předchozích letech, kdy takto bezprecedentní nárůst nebyl zaznamenán.




*Graf 12 Vývoj indexu TČ hlavy X TZK [40]*

Pro výpočet indexu finančních škod způsobených kybernetickou kriminalitou byla jako nejvhodnější zvolena mocninná trendová funkce. Metodou nejmenších čtverců byly odhadnuty parametry rovnice mocninné trendové funkce ve tvaru „$y = a*t_i^b$“ jako „a = 584876“ a „b = 1,215“. Po dosazení těchto parametrů do rovnice byly spočítány hodnoty prognózy vývoje indexu finančních škod pro rok 2019 na 8 442 319, v roce 2020 by index měl dosahovat hodnoty 9 595 268 a v roce 2021 by se měl zvýšit až na 10 773 312. Index determinace pak pro mocninnou funkci činil 0,8978, index korelace dosáhl hodnoty 0,9278 a střední absolutní procentuální chyba odhadu dosáhla nejvyšší hodnoty ze všech posuzovaných kategorií, a to 30 %. Evidentně je tak díky velkým výkyvům tato prognóza velmi hrubým odhadem toho, jak by se v budoucnu mohly vyvíjet finanční škody způsobené kybernetickou kriminalitou. Avšak i přes členitost křivky ve sledovaném období se mocninná trendová funkce nakonec ukázala jako nejvhodnější metodou stanovení odhadu. Budeme-li předpokládat stejný počet obyvatel na území České republiky, mohly by v roce 2021 celkově způsobené finanční škody kybernetickou kriminalitou

dosáhnout 1,147 mld. Kč. To by znamenalo, že bazický index dosáhne v roce 2021 hodnoty 1337 % oproti škodám způsobeným v roce 2011. V porovnání s předpokládaným bazickým indexem v roce 2021 v rámci registrovaného počtu trestných činů, který by měl dosahovat 591 % je rozdíl v tempu růstu více než dvojnásobný.




*Graf 13 Vývoj indexu finančních škod způsobených kybernetickou kriminalitou [40]*

## 5.4 Dopady kybernetické kriminality na obyvatelstvo

Dopady kybernetické kriminality na obyvatelstvo mohou být různé. V rámci této práce si je rozdělíme na dopady ekonomické, psychologické a společenské. V rámci stanovení dopadů budeme vycházet z výše uvedených analyzovaných statistik druhů kybernetické kriminality.

### 5.4.1 Ekonomické dopady

Ekonomické dopady kybernetické kriminality nepůsobí pouze na jednotlivce, ale v závislosti na činu i na různé instituce nebo stát. Obecně ekonomické dopady kybernetické kriminality znamenají zejména způsobení finančních škod čili ztrátu finančních prostředků, nebo například u porušování autorského zákona ušlý zisk.

V případě ekonomických dopadů na fyzické osoby, které se staly obětí kybernetické kriminality, dochází ke škodám zejména kvůli odcizení finančních prostředků. V rámci statistik počtu trestných činů, kde majoritní část kybernetické kriminality, u kterých byla stanovena finanční škoda, jsou trestné činy, kdy se škody pohybují od 5000 do 10 000 Kč, předpokládáme, že se jedná o trestnou činnost orientovanou na jednotlivce. U této trestné činnosti dojde například ke krádeži virtuální identity a následnému obohacení pachatele pomocí získaných informací. Ty pak mohou být využity k čerpání finančních prostředků, které oběť již vlastní nebo k jejich získání na pomocí ukradené virtuální identity a vytvořením škod, které na oběť dopadnou. U phishingových útoků, které jsou využívány buď k přímému vylákání finančních prostředků nebo získání přihlašovacích údajů, mohou být způsobeny škody po nainstalování programů typu malvare nebo ransomware poškozením samotného zařízení. V případě využití malware, který vytvoří ze zařízení bot v botnet síti s následným využíváním výpočetního potenciálu a zvyšováním výkonu, pak teoreticky snižuje životnost napadeného zařízení. Dále tato činnost zvyšuje například i odběr elektrické energie nebo čerpá data, která způsobují finanční škodu v případě, že oběť platí svému poskytovateli internetu za objem vyčerpaných dat. Nepředpokládáme, že tento druh škod je zahrnut ve statistikách PČR, ale předpokládáme, že k nim dochází. Jestliže je zařízení oběti napadeno programem typu ransomware, dochází ke škodám v několika variantách. Za prvé v případě přistoupení na podmínky pachatelů a odeslání požadovaných finančních prostředků. Druhá varianta ekonomické škody je pak nutné vyhledání servisního centra a zaplacení služeb, potřebných

k odstranění ransomware ze zařízení. K této variantě může dojít i když oběť přistoupí na požadavky pachatelů, ti často zařízení i přes zaplacení neodemknou. A poslední variantou je pak škoda v rámci ztráty uložených dat v případě, že ransomware mazal nebo uzamykal uložiště zařízení. Všechny tyto varianty jsou navzájem kombinovatelné.

Zaměříme-li se na různé instituce, právnické osoby a podnikající fyzické osoby (dále právnické osoby) dojdeme k závěru, že varianty škod zmíněné v rámci jednotlivce jsou aplikovatelné i na tuto kategorii. V případě ekonomických dopadů, které působí na právnické osoby, se ukázalo, že často páchaným trestným činem je porušování § 211 - Úvěrový podvod. V roce 2018 bylo spácháno 891 úvěrových podvodů, přičemž jich bylo objasněno 630. Dohromady byly způsobeny škody za 39 211 729 Kč. Domníváme se, že nejčastěji dochází ke spáchání úvěrových podvodů v oblasti kybernetické kriminality právě za použití odcizených virtuálních identit. V ten moment vznikají škody nejen právnickým osobám, ale také mohou vzniknout jednotlivcům, jejichž identita byla použita na sjednání určeného úvěru.

Průmyslová špionáž může v konečném součtu způsobit obrovské finanční ztráty, pokud dojde například k odcizení patentu nebo jiných informací, které jsou pro napadenou společnost důležité. Předpokládáme, že PČR hodnotí průmyslovou špionáž jako porušení § 230 – Neoprávněný přístup k počítačovému systému a nosiči informací při naplnění znaků porušení odstavce *„4e-způsobí-li takovým činem vážnou poruchu činnosti právnické nebo fyzické osoby“*. Trestných činů naplňujících tento odstavec bylo registrováno v roce 2018 dohromady 26. Ani jeden z těchto činů nebyl objasněn, 17 jich nezpůsobilo žádné škody a zbylých 9 trestných činů způsobilo škody dohromady za 5 855 891 Kč, přičemž největší škody v rámci jednoho trestného činu činily 5 101 000. Pro porovnání v roce 2016 byly takto evidovány pouze 3 trestné činy s celkovou škodou 5000 Kč, a v roce 2017 bylo evidováno 9 trestných činů, z nichž 6 nezpůsobilo žádné škody a zbylé tři

dohromady způsobily škody v hodnotě 4 425 673 Kč, z toho 4 308 000 Kč spáchal pouze jeden trestný čin. PČR nedokázala objasnit ani jeden z těchto trestných činů způsobených právnickým osobám.

Ekonomické dopady způsobené porušováním autorského zákona jsou hlavně v souvislosti s ušlými zisky. Porušováním autorského zákona vznikly v roce 2018 škody v rozsahu 111 044 440 Kč. V tomto roce bylo evidováno 498 skutků, z nichž bylo 320 objasněno. Největší škoda byla způsobena částkou 53 158 905 Kč. Při škodách takového rozsahu způsobených autorům investujícím velké částky do díla, kdy se počítá s návratností této investice, mohou takové okolnosti značně poškodit jejich další tvorbu a konkurenceschopnost v prostředí jejich podnikání.

Na stát jsou rovněž přenositelné stejné dopady, které byly nastíněny výše, stanou-li se v souvislosti s jeho zařízeními, systémy nebo úřady. Pokusíme-li se zhodnotit přímé dopady na státní aparát, jedná se o finanční výdaje spojené s nápravou škod po útocích na systémy státní správy, jimiž mohou být DDoS útoky, neoprávněné přístupy nebo jiné formy kybernetické kriminality postihující systémy a zařízení státní správy. Ač PČR neuvádí škody spojené s porušením § 357 – Šíření poplašené zprávy, za rok 2018 bylo evidováno 48 takových skutků, přičemž 25 jich bylo objasněno. Je zřejmé, že ekonomické dopady spojené s touto trestnou činností jsou hlavně v rámci manévrů složek IZS, které tuto poplašnou zprávu musí prověřit. PČR ve svém článku uveřejnila náklady na prověření anonymu, který nahlašuje výbušné zařízení. Tyto náklady jsou v článku vyčísleny na příkladu nahlášení bomby v restauračním zařízení na 44 920 Kč. [42] tato částka se samozřejmě zvyšuje, je-li poplašná zpráva nahlášena například v obchodním centru nebo na letišti. Výše uvedená částka stále nezapočítává škody, které vzniknou subjektu, kde je poplašná zpráva nahlášena. Tyto škody jsou pak velmi variabilní.

### 5.4.2 Psychologické dopady

Psychologické dopady, které může mít kybernetické kriminalita na jedince se různí. Budeme-li uvažovat o psychologických dopadech v rámci trestné činnosti, která oběti způsobí ekonomické škody, může se oběť v rámci svého rozpočtu dostat do svízelné ekonomické situace, díky které prožívá emoční stres a nejistotu. Taková situace může ve vážných situacích přerůst až v deprese a v případě závažných ekonomických problémů, které se pro oběť zdají být neřešitelné se mohou objevit i suicidální myšlenky.

Kybernetická trestná činnost, která porušuje paragrafy v rámci hlavy III je nejvíce propojena s výrobou a distribucí dětské pornografie. Dopady na děti, které jsou zneužívány k výrobě těchto materiálů nejsou nijak blíže prozkoumány. Pierce se ve svém článku domnívá, že dětská zranitelnost je do značné míry udávána jejich neschopností zpracovat fyzické, psychologické a emocionální aspekty takového zážitku. Pocity, které obecně mohou tyto oběti zažívat, jsou pocity zrady, viny, bezmoci a vzteku. Jeden z nejhorších dopadů na tyto oběti je ale v tom, že lidé, kteří byli v dětství zneužíváni, mají následně v životě tendence k tomu, aby také v dospělosti zneužívali děti. [43] Dále můžeme vycházet z obecných předpokladů toho, jaké má sexuální zneužívání dopad na dětské oběti, k čemuž v rámci kybernetické kriminality svědčí trestné činy spadající pod § 192, § 193 a § 202. Děti, které zažívají sexuální týrání od útlého věku, jsou ve svém vývoji opožděné, přičemž jejich chování vykazuje známky sexuální agresivity, bývají apatické a rigidně ostražité. Jakmile dítě začne zažívat sexuální zneužívání, začíná se u něj objevovat zhoršení komunikace, je vzpurné, zhorší se mu školní prospěch a objevují se u něj další známky patologických jevů, jako záškoláctví nebo útěky z domova. Důsledkem takového zneužívání bývá rozvoj Postraumatické-stresové poruchy a u obětí se objevují suicidální myšlenky, případně pokusy o suicidum. [44]

Závažné psychologické dopady mohou způsobovat obětem trestné činy v rámci § 353 a § 354, které řadíme v rámci kybernetické kriminality pod kyberstalking. Přestože stalking může vygradovat až do fyzického násilí, nezanedbatelné dopady má pro oběti zvláště dlouhodobý stres a strach z fyzického násilí. V rámci tohoto stresu se pak u obětí častěji objevují chronická onemocnění jako bolesti zad nebo deprese. Vzhledem ke standardizované léčbě těchto onemocnění pomocí analgetik a antidepresiv může docházet k závislosti na daných substancích a výrazné ovlivnění kvality života i po tom, co stalking skončí. Osoby, u kterých se objeví výše zmíněná onemocnění se musí potýkat se sníženým finančním příjmem v rámci léčení těchto chorob nebo se snížením pracovního výkonu, což může vést až ke ztrátě zaměstnání. [45]

U trestných činů proti § 355 a § 356 vycházíme z psychologických dopadů osob, které zažívají rasismus. Oběti těchto trestných činů prožívají stres, pocity strachu vůči jiným skupinám osob, bezmoci a takové stresory mohou vyústit až v deprese nebo vývoj jiných chronických onemocnění, u kterých je dlouhodobý patologický stres rizikovým faktorem. [46]

### 5.4.3 Společenské dopady

Společenské dopady kybernetické kriminality můžeme odvozovat z dopadů na fyzické a právnické osoby a rozebrání jejich vlivu na společnost jako takovou. Určité dopady na společnost s sebou nesou i opatření, která stát a mezinárodní organizace uplatňují v rámci kontroly kybernetické kriminality. V poslední době se můžeme bavit o článku 13 (ve finálním číslování posunuto na číslo 17) z nové *„Směrnice o harmonizaci některých aspektů práva autorského a práv souvisejících v informační společnosti“*, kterou schválila Evropská unie. Tato směrnice má za cíl lépe chránit autorská práva. Ovšem velkou kritiku sklidil právě článek 13, kdy se veřejnost a odborníci obávají z plošné cenzury na internetu. Tato „cenzura“ má probíhat tak, že každý střední nebo větší poskytoval služeb na internetu (např.

Google, Facebook, Youtube) má povinnost hlídat autorské právo za autory. Technologicky to znamená zavedení systému, který bude ověřovat každý nahraný obsah s databází a jakmile objeví shodu, která je v rozporu s autorským zákonem, tento obsah zablokuje. Částečně už tyto mechanismy fungují zvláště na platformě Youtube, kam se uživatelé snaží nahrávat například filmy. Strach z masového nasazení této technologie pramení hlavně z důvodu, že se kontrola nebude týkat pouze celého díla, ale také všech fragmentů, citací nebo satiry. Tento mechanismus tak může ovlivnit žurnalistiku a svobodu slova jednoduše tím, že jakmile systém nalezne shodu, při vyhledávání (v případě Google) se prostě nezobrazí. Google s touto technologií provedl experiment a zveřejnil, že i při umírněné verzi tohoto systému došlo k 45% redukci návštěvnosti novinářských stránek. [47] Nutno podotknout, že tato opatření se zavádí zvláště kvůli masivnímu porušování autorských práv na internetu a s tím spojenými finančními škodami pro autory.

V případě porušování § 355, § 356 a v návaznosti § 403 a § 404 může dojít k ovlivnění dalších osob a jejich sympatizování s takovými lidmi nebo skupinami. Tyto skupiny pak mohou i za pomocí šíření poplašných zpráv (§ 357) vyprovokovat násilí na skupinách obyvatelstva. Podobný případ se odehrál ve Francii, kdy falešná zpráva o tom, že francouzští Romové unášejí děti, vyvolala hromadné násilí na několika místech v zemi, směřované právě proti Romům. [48] Při kumulaci takových zpráv a případů dochází u uživatelů internetu k tomu, že bývají často zmateni a při nedostatečném ověření informací, které si na internetu přečtou, se mohou rozhodnout k vykonání podobně motivovaného skutku. Tento informační balast může ve výsledku vést i k radikalizaci části populace. Kvůli možnosti publikování dezinformací a ovlivňování veřejného mínění může teoreticky dojít k vyvolání nepokojů a k ovlivnění volebních výsledků, což může mít za následek dosazení lidí do státní správy, kteří budou pracovat ve prospěch jiné mocnosti a tím i destabilizaci státu. V případě, že stát nebude schopen před kybernetickou kriminalitou chránit své občany a vlastní struktury, může dojít

k vyvolání nedůvěry společnosti v bezpečnostní složky a právní systém, který boj s kybernetickou kriminalitou prohrává.

## 5.5 Doporučení na obranu proti kybernetické kriminalitě

Doporučení na obranu proti kybernetické kriminalitě se budou vztahovat k tomu, jak by se měl chovat jedinec v kybernetickém prostředí, jaké kroky by měly podniknout právnické osoby v rámci obrany proti kybernetické kriminalitě a jak může stát pomoci tomu, aby se co nejvíce eliminovala rizika v kybernetickém prostoru a jak může docílit zefektivnění potírání tohoto druhu kriminality.

K tomu, aby fyzické osoby co nejvíce snížily riziko plynoucí z kybernetické kriminality je zapotřebí základní znalost kybernetického prostoru, technik zločinců, dostatečné technické zabezpečení vlastního zařízení a používání kritického myšlení. Základním stavebním kamenem obrany je tedy znalost. Vzděláváním populace můžeme zamezit rizikovému chování na internetu a tím razantně snížit šance zločinců na úspěch v jejich snažení. Takové vzdělávání je okrajově zahrnuto na základních školách rámci hodin informatiky. Ke zkvalitnění této výuky je zapotřebí mít zejména kvalitně proškolené učitele, přednášející tuto tématiku a zanesení výuky bezpečného chování v kyberprostoru do učebních osnov. Vzhledem k tomu, že se na internetu pohybují stále mladší děti, je zapotřebí s tímto vzděláváním začít hned, jak je to možné. V rámci této výuky by se žák měl seznámit s principy, jak nakládat se svými daty, jak by měl přistupovat ke sdílení citlivých informací na sociálních sítích, naučit se kritickému myšlení při vyhledávání informací a zásady bezpečné komunikace.

I přes to by měli rodiče kontrolovat, jak se jejich dítě na internetu chová. K tomu jsou již dnes k dispozici programy rodičovské kontroly, které jsou součástí operačního systému Windows, nebo jsou nabízeny v rámci placených verzí antivirových programů. Dokonce platformy, na kterých mládež tráví nejvíce času (Youtube, Facebook) poskytující rodičům možnost kontrolovat jaký obsah se jim

zobrazuje. Je nutné podotknout, že jestliže je dítě technicky zdatnější než jeho rodič, nebude mu dělat velký problém tyto mechanismy obejít. Je proto důležité, aby dítě chápalo, jaké nástrahy ho na internetu čekají a jaké následky může nezodpovědné chování na internetu přinést. Takovou výchovu nemůže dostatečně obsáhnout školní vyučování, ale musí se doplňovat s výchovou z domácího prostředí.

Aby mohli rodiče učit své děti bezpečnému chování na internetu, je zapotřebí aby oni sami znali rizika plynoucí z pohybu v kybernetickém prostředí. Systémová výuka generace, která již je ze školních lavic pryč je nereálná. Edukace této části populace, by tak měla probíhat skrze informační kampaně podobným způsobem jakým jsou prováděny informační kampaně pro bezpečnost silničního provozu v rámci BESIP. Podobné informační kampaně již probíhají i dnes. Nedostává se jim ale dostatečného mediálního prostoru k oslovení větší části populace.

Důležitost přítomnosti kritického myšlení a ověřování informací ukazuje i fakt, že nejčastějším trestným činem v rámci kybernetické kriminality je podvod. Pouze trestné činy spadající pod § 209 měl podíl 47 % z celkové kybernetické kriminality. Phishing, u kterého se domníváme, že se velkou mírou podílí na tomto druhu kriminality, je možné velice efektivně odhalit, právě díky kritickému myšlení. Phishingové útoky totiž často postrádají dostatečnou kvalitu k tomu, aby je i oko laika nedokázalo odhalit. Je důležité populaci upozorňovat na probíhající vlny phishingových útoků pomocí massmédií. Společnost, která má povědomí o takové trestné činnosti jí spíše nepodlehne. Kritické myšlení ovšem neslouží jen k odhalování podvodů. Díky ověřování informací je uživatel následně schopen rozeznat fake news a šíření poplašných do zpráv do jejichž kategorie by se některé dezinformace daly zařadit. Čím více bude populace schopna rozeznat dezinformace šířící se na internetu, tím spíše je chráněna od negativních aspektů těchto zpráv, jako je ovlivnění mínění nebo v extrémním případě i radikalizace a negativní jevy z ní plynoucí.

Pro zabezpečení zařízení, která jsou připojena k internetu existuje řada bezplatných antivirových programů, které jsou schopny ochránit proti virům a malware. Bezplatné antivirové programy dokonce mají stejnou databází vzorků jako jejich zpoplatněné verze. Je pak na každém, jak se rozhodne investovat do své ochrany. Placené antivirové programy nabízí řadu dalších možnosti, jak se chránit na internetu jako ochranu proti phishingu, spamu nebo zabezpečení bankovních transakcí. Důležité je mít v zařízení nainstalovaný alespoň nějaký druh antivirového programu, protože základní ochrana, která je součástí operačních systémů není dostatečná. To se týká nejenom počítačů, ale také tabletů a telefonů, na které běžní uživatelé často zapomínají.

Právnické osoby a subjekty, které využívají v rámci svojí činnosti počítačové systémy a interní sítě, by měly dbát na dostatečnou edukaci zaměstnanců, kteří s nimi pracují. Edukace a vzdělání těchto zaměstnanců v oblasti počítačové bezpečnosti je nejlepší ochranou proti infikování takových systému škodlivým softwarem a následnému poškození sítě, zařízení nebo úniku citlivých informací. V rámci těchto sítí lze využít monitorovací systémy chování uživatelů v síti a aktivně tak vyhledávat rizikové zaměstnance, u kterých hrozí, že by mohli být zdrojem nebezpečí. Stejně důležité jako edukace zaměstnanců je u rozsáhlejších sítí také jejich technologické zabezpečení. Subjekty k jejichž činnosti patří i uchovávání citlivých informací, ať už o jejich činnosti nebo o jejich klientech (např. nemocnice, pojišťovny, úřady atd.), musí být odolné i proti cíleným útokům na jejich kybernetickou infrastrukturu. Je důležité, aby tyto subjekty pravidelně testovaly odolnost jejich zabezpečení proti hackerským aktivitám a tím zabránily dalším škodám. Takové testování pak může provádět IT oddělení daného subjektu nebo je možnost zaplacení služeb externí firmy specializující se na bezpečnost informačních systémů, aby takové testování provedla a případně doporučila další opatření vedoucí k zajištění maximální bezpečnosti.

Stát by měl k hrozbám plynoucí z kybernetického prostředí přistupovat velmi vážně. Systémových opatření, která může provádět v rámci své činnosti je několik. Jako první, jak jsme zmiňovali výše, je zajištění vzdělání a edukace obyvatelstva, aby vědělo, jak se na v kybernetickém prostoru chovat. Toto vzdělávání je okrajově pro nejmladší generaci zavedeno již na základních školách, zlepšení může stát docílit úpravou školních osnov pro školní zařízení. Tato výuka by neměla být omezena pouze na žáky základních škol, ale měli by se jí věnovat i studenti středních škol a odborných učilišť jako riziková skupina. V rámci takového rozsahu výuky by mělo být zajištěno proškolení vyučujících pedagogů na téma kybernetické bezpečnosti. Pro edukaci starší populace je možnost vytváření informačních kampaní upozorňující na negativní jevy v kybernetickém prostoru. Tuto činnost by mohl zajišťovat subjekt zřízený pod příslušným ministerstvem, v podobném principu jako funguje BESIP pod Ministerstvem dopravy. Nabízí se možnost tuto činnost převést na Centrum proti terorismu a hybridním hrozbám fungujícím pod Ministerstvem vnitra. Toto centrum má již nyní, v rámci pracovní náplně přicházet s návrhy na legislativní úpravy, sledování poplašných zpráv a dezinformací souvisejících s vnitřní bezpečností státu a jistě disponuje odborníky, kteří jsou schopni odborně takové kampaně zaštiťovat. Jestliže není možné, aby se stát zajímal i o obecný fact checking (ověřování informací), a snažil se potvrzovat nebo vyvracet informace kolující v internetovém prostředí, může formou dotací, podporovat již zaběhlé platformy v tomto odvětví a kontrolovat jejich nezávislost.

U technologického zabezpečení musí stát udržovat ochranu svých počítačových sítí na maximální možné úrovni. Kontrolu této ochrany by měl provádět na základě nezávislých auditů a testování a výsledky těchto kontrol zahrnout do dalších postupů v zabezpečení. Zvláště by se měl věnovat kybernetické ochraně kritické infrastruktury, u které hrozí, že se na ni útočník v případě, že by chtěl způsobit co největší škody, zaměří. U prvků kritické infrastruktury, které nejsou ve vlastnictví státu, by pak měl vykonávat pravidelné kontroly tohoto zabezpečení a požadovat po subjektu vlastnícím prvek kritické infrastruktury zajištění co nejvyšší

úrovně kybernetické ochrany. Tyto aspekty ochrany upravuje Krizový zákon č. 240/2012 Sb. a Zákon o kybernetické bezpečnosti č. 181/2014.

Stát by měl také co nejefektivněji upravovat legislativu na základě nejnovějších mezinárodních trendů, a to jak v oblasti kybernetické bezpečnosti, tak i trestního práva. Měl by do svého právního řádu, také včleňovat směrnice a doporučení z Evropské unie. V oblasti autorského zákona, kdy u jeho porušování dochází k vysokým škodám, které jsou způsobeny autorům zejména u pirátských aktivit na internetu, se nabízí kontrola obsahu datových uložišť jako je například Ulož.to nebo Hellspy, jejichž obsah z větší části právě autorský zákon porušuje a na základě nabízených služeb nahrávání a stahování pirátského obsahu tyto platformy získávají finanční prostředky. Jestliže takový subjekt není schopen zjednat nápravu a odstraňovat tento obsah ze svých uložišť, měl by nést částečnou odpovědnost za to, k čemu jej jeho klienti využívají. Tato opatření by ale měla být směřována právě na datová uložiště, ze kterých dochází ke stahování obsahu nikoliv na poskytovatele internetových služeb v rámci vyhledávání jako je Google, kdy zavedení takových nástrojů nepřinese kýžený efekt, vzhledem k tomu, že populace, která služby datových uložišť ke stahování pirátského obsahu využívá tyto platformy k jeho vyhledání nepotřebuje. Tímto by došlo k došlo selekci veškerého obsahu, který by systém vyhodnotil duplikující nebo kopírující, což nemusí být vždy pravdou. Cestou je i blokace stránek jim podobným, jako je například The Pirate Bay, jenž poskytuje torrentové soubory ke stahování pirátského obsahu. Tento krok posvětil Soudní Dvůr Evropské unie v roce 2017 a poskytovatelé internetu tak mohou například právě The Pirate Bay blokovat. Blokace každé stránky, která by mohla porušovat autorská práva musí předcházet podrobná analýza a mělo by se tak dít za rozhodnutí nezávislého soudu, aby nedocházelo k pokusům o cenzuru v internetovém prostředí.

K tomu, aby bezpečnostní složky byly schopné efektivně potírat kybernetickou kriminalitu, je za potřebí aby jejich příslušníci měli odpovídající vzdělání v oblasti

kybernetické bezpečnosti, dostatečné technické zázemí a personální zajištění. K tomu, aby měli policisté vyšetřující kybernetickou kriminalitu šanci udržet s pachateli krok, potřebují mít k dispozici to nejmodernější vybavení, které je právě pachateli využíváno. Při jeho absenci pak výrazně klesá šance na jejich dopadení. V rámci těchto opatření by mělo být investováno do pravidelné údržby a obnovy tohoto technického vybavení. Důležité je také vzdělávání všech příslušníků, kteří se s kybernetickou kriminalitou setkávají. Již dnes je v rámci každého Krajského Policejního ředitelství zřízen odbor kybernetické kriminality. Specialisté z těchto odborů by měli zajišťovat edukační činnost pro své kolegy na územních odborech, aby i oni byli schopni kybernetickou kriminalitu v rámci své působnosti objasňovat. K tomu, aby tyto odbory získaly potřebné odborníky je potřeba, aby Policie ČR byla konkurence schopným zaměstnavatelem soukromému sektoru. K tomu může sloužit zejména lepší nabídka platového ohodnocení, zaměstnaneckých benefitů nebo náborových příspěvků. Žádoucí je také nepřetržité sledování vývoje trendů kybernetické kriminality v rámci celého světa ve spolupráci s nadnárodními bezpečnostními složkami jako Interpol a Europol další školení, vzdělávání a vzájemného předávání získaných poznatků. K tomu, aby příslušníci Policie ČR byli schopni objasňovat kybernetickou kriminalitu, je potřeba mít zavedenou spolupráci na dostatečné úrovni s poskytovateli internetu a poskytovateli služeb na internetu. Tyto subjekty mohou být nezastupitelným pomocníkem v rámci vyšetřování kybernetické kriminality.

# 6 DISKUZE

Cílem této práce bylo vypracovat analýzu na registrovanou kybernetickou kriminalitu na území České republiky. Tato analýza byla provedena v části popisné, kde byly popsány statistiky již zaregistrované kybernetické kriminality. Druhá část se věnovala prognóze možného vývoje kybernetické kriminality. Některé z těchto prognóz vykazují nižší míru spolehlivosti, což je v práci popsáno a tento jev je zapříčiněn hlavně členitostí získaných dat.

Analýza kybernetické kriminality v rámci praktické části této práce potvrdila všechny hypotézy, které byly stanoveny. Zaměříme-li se na první hypotézu, dojdeme k závěru, že ekonomicky orientovaná trestná činnosti, která je zahrnuta pouze pod hlavou V činní podíl této činnosti 69 % z celkového počtu. Přičteme-li k tomu i registrované skutky v rámci hlavy VI dostaneme se na celkový podíl 80 %. Celkový podíl ekonomicky orientované trestné činnosti je mnohem vyšší, než se původně předpokládalo. Je velice pravděpodobné, že registrovaný počet skutků tohoto charakteru nereflektuje přesný počet této trestné činnosti. Předpokládá se, že oběti často nenahlásí trestný čin s nižší způsobenou škodou. To z části může reflektovat i podíl nahlášených skutků se způsobenou finanční škodou menší než 5000 Kč.

Z analýzy počtů registrovaných skutků se potvrdila i druhá hypotéza, která předpokládala, že průměrný meziroční nárůst registrovaných skutků v rámci kybernetické kriminality bude činit alespoň 20 %. Tento nárůst nakonec činil 26 % ve sledovaném období. Z otevřených zdrojů lze zjistit, že v Kanadě proběhl nárůst kybernetické kriminality v letech 2014 - 2016 o 45 %, v tomto období v České republice narostla kybernetická kriminalita o 14 %. Japonsko zase v roce 2017 zaznamenalo rekord, kdy bylo zaznamenáno 70 000 trestných činů v rámci kybernetické kriminality. [49] Při stejném výpočtu indexu skutků, jaký jsme používali v rámci analýzy dostaneme výsledek 55,2. Ten je tak téměř shodný

s indexem téhož roku v ČR, který činil 53,4. Zahrneme-li do toho porovnání například ještě Belgii, která je populačně podobně veliká jako ČR, zjistíme, že v Belgii je počet registrovaných skutků mnohonásobně vyšší. Jejich index s 20 528 registrovanými skutky v roce 2017 činil neuvěřitelných 180,9. [50] Tak vysoké číslo může ukazovat opravdu na mnohonásobně vyšší počet kybernetické kriminality v této zemi, nebo také na vyšší zájem bezpečnostních složek v rámci vyšetřování tohoto druhu kriminality.

Při sledování vývoje bazického indexu a vytvářením jeho prognózy na období dalších 3 let pomocí polynomické trendové funkce, který určuje celkový procentuální nárůst oproti začátku sledovaného období, jsme potvrdili třetí hypotézu, která předpokládala, že v prognóze na další 3 roky proběhne nárůst kybernetické kriminality o více než 500 % oproti roku 2011. V rámci této trendové funkce by se měl bazický index přehoupnout přes 500% hranici již v roce 2019 s prognózou 502 % a v roce 2021 by měl dosahovat 591 %. Tato prognóza se jeví jako reálná vzhledem k vypočteným indexům k určení vhodnosti funkce a střední absolutní procentuální chyby dosahující 6 %. Porovnáme-li vývoj kybernetické kriminality v ČR s vývojem z Belgie, tak v Belgii činil bazický index v roce 2017 30 % oproti roku 2011. Nutno podotknout, že z Belgie jsou k dispozici data o kybernetické kriminalitě již z roku 2007, kdy měli vyšší počet registrovaných skutků než Česká republika v roce 2018. [50] Nepředpokládáme tak vysoké rozdíly v intenzitě kybernetické kriminality v rámci dvou geograficky a populačně podobných zemích, ale spíše v rozdílech aktivity proti kybernetické kriminalitě a procesních záležitostí v rámci bezpečnostních složek daných zemí.

U analýzy výše způsobených škod můžeme Českou republiku porovnat se Spolkovou republikou Německo, kde kybernetická kriminalita v roce 2016 způsobila škody ve výši 51 mil. €. [51] Při přepočtu na koruny vzhledem k průměrnému kurzu za rok 2016, který činil 27,033 Kč vycházejí škody na 1,4 mld. Kč. [52] Při porovnání indexů vzniklých škod mezi Spolkovou republikou

Německo a Českou republikou dojdeme k zajímavému rozdílu. Index škod v Německu činil v roce 2016 1 665 277, kdežto v ČR byl 7 076 369. Tento rozdíl je zapříčiněn tím, že v Německu do těchto škod nebyly nezapočítávány škody, které byly způsobeny společnostem. Jestliže by se započítala i škoda způsobená společnostem, odhadují se škody na 22,4 bil. €. [51] Celosvětově se škody spojené s kybernetickou kriminalitou vyčíslují za rok 2017 na 600 bil. $. [49] Čtvrtá hypotéza této práce předpokládala, že se v prognóze zvýší objem způsobených škod kybernetickou kriminalitou na území České republiky nad hranici 1 mld. Kč. Tato hypotéza byla potvrzena předpokládaným zvýšením škod na 1,147 mld. Kč. Trendová funkce, která byla použita na předpovězení trendu růstu škod ovšem vykazovala nejnižší vypočtené hodnoty pro určení vhodnosti zvolené funkce z všech vypracovaných funkcí a se střední absolutní procentuální chybou 30 % ukazuje pouze hrubý odhad předpokládaného vývoje. Data, která byla použita pro výpočet této funkce totiž vykazovala vysokou kolísavost a není možné tak předpovědět vývoj objemu finančních škod s vyšší přesností.

Společenské a ekonomické dopady byly odvozeny v závislosti na předpokládané trestné činnosti a možných scénářích následujícího průběhu. Tyto scénáře zohledňují typologii trestného činu a míry škod, které může v teoretické rovině napáchat. Platí, že se scénáře a celkové dopady mohou lišit v závislosti na specifikách trestné činnosti a oběti. Tyto dopady jsou vyhodnoceny na základě zjištěných a nastudovaných skutečností v rámci výzkumu této práce, ovšem nejsou opřeny o již proběhlé studie na podobné téma. Hodnocení psychologických dopadů kybernetické trestné činnosti vychází ze studií psychologů u obětí stejných trestných činů nebo jim velmi podobným, které ale nebyly prováděny specificky na tyto patologické jevy v rámci kybernetického prostředí. Tyto dopady mohou být odlišné v závislosti na typologii oběti a specifikům průběhu dané trestné činnosti.

Doporučení pro obranu proti kybernetické kriminalitě vypracovaná v této práci vychází zejména z obecných zásad ochrany proti kybernetické kriminalitě a

pohybu v kybernetickém prostoru. Tyto obecné zásady byly rozpracovány do kroků, které může podniknout fyzická osoba, právnická nebo podnikající fyzická osoba a stát. Není nikde popsáno, jak moc jsou v rámci fyzických nebo právnických osob popsané možnosti ochrany využívány. U doporučení, která by mohl provádět stát nebyly nalezeny dokumenty, které by popisovaly úroveň zabezpečení úřadů nebo prvků kritické infrastruktury. Vycházíme tedy z krizového zákona č. 240/2000 Sb. a zákona o kybernetické bezpečnosti č. 181/2014 Sb., který zmíněnou právní úpravu již obsahuje. Při popisu doporučení pro úpravu autorského zákona a ochrany autorů jsou brány v úvahu již zavedené nebo zavádějící se mechanismy a jejich možné úpravy k dosažení co nejvyšší efektivity v kombinaci s co nejmenší mírou jakékoli formy cenzury nebo omezení svobody slova. Doporučení popsaná v části věnované bezpečnostním složkám vychází z obecně známých problémů, se kterými se Policie ČR potýká a možnými scénáři řešení, jak tuto situaci zlepšit. Předpokládá se, že doporučená spolupráce v rámci ostatních subjektů a bezpečnostních sborů probíhá již v současnosti, ale není jasné, na jaké úrovni a v jaké intenzitě.

# 7 SEZNAM POUŽITÝCH ZKRATEK

AT&T – American Telephone and Telegraph

ARPA - Advanced Researsch Project Agency

BBN – Bolt, Beranek, Newman Technologies

CD - Compact Disc

ČR - Česká republika

DARPA - Defence Advanced Researsch Project Agency

DDoS - Distributed Denial off Service

DMS - Dárcovská SMS

DNS - Domain Name System

Doc - Document

DoS - Denial of Servise

DRDoS - Distributed Reflection Denial of Service

DVD - Digital Versatile Disc

EC3 - European Cybercrime Centre

EFF – Electronic Frontier Foundation

EULA - End User License Agreement

FBI – Federální úřad pro vyšetřování

GBps - Gigabytes Per Second

IBM - International Business Machines

ICMP - Internet Control Message Protocol

IOT - Internet of Things

ISO – Mezinárodní organizace pro normalizaci

IP - Internet Protocol

IPv4 - Internet protocol version 4

IPv6 - Internet protocol version 6

ISP - Internet Service Provider

IT - Informační technologie

J - CAT - Joint Cybercrime Action Taskfroce

Kč - Koruna česká

KGB – Výbor státní bezpečnosti

LAN - Local Area Network

MAC - Media Access Control Address

MAN - Metropolitan Area Network

MIT - Massachusetts Institute of Technology

NAT - Network address translation

NCOZ – Národní centrála proti organizovanému zločinu

NSF - National Science Foundation

NÚKIB - Národní úřad pro kybernetickou a informační bezpečnost

OS - Operační systém

P2P - Peer to peer

PAN - Private Area Network

PC – Osobní počítač

PIN - Personal Identification Number

RAM - Random Access Memory

SKPV – Služba kriminální policie a vyšetřování

SMS - Short Message Service

TBps - Terabytes Per Second

TCP - Transmisssion Control Protocol

TČ – Trestná činnost

TZK – Trestní zákoník

USB - Universal Serial Bus

VPN - Virtual Private Network

WAN - Wide Are Network

# 8 SEZNAM POUŽITÉ LITERATURY

[1] BAETA, Maria. All about Creeper, the first virus in history. *Softonic* [online]. 30.8.2017 [cit. 2018-11-30]. Dostupné z: https://en.softonic.com/articles/all-about-creeper-the-first-virus-in-history

[2] KOVALCHIK, Kara. TRUE CRIME: John Draper, the original whistle blower. *Mental Floss* [online]. 30.8.2008 [cit. 2018-11-30]. Dostupné z: http://mentalfloss.com/article/19484/true-crime-john-draper-original-whistle-blower

[3] A Brief History of Cyber Crime. *Florida Tech* [online]. [cit. 2018-11-30]. Dostupné z: https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/

[4] GIBSON, William. *Neuromancer*. Plzeň: Laser, 1992. Golden Sci-Fi. ISBN 80-856-0127-3.

[5] BARLOW, John. Declaration of the Independence od Cyberspace. *Electronic Frontier Foundation* [online]. 2.8.1996 [cit. 2018-12-03]. Dostupné z: https://www.eff.org/cyberspace-independence

[6] KRAMER, Franklin, Stuart STARR a Larry WENTZ. Cyberpower and National Security. *National Defence University Press* [online]. 1.4.2009 [cit. 2019-04-07]. Dostupné z: https://ndupress.ndu.edu/Media/News/Article/1216674/cyberpower-and-national-security/

[7] ISO/IEC 27032:2012: Guidlines for security. *ISO Online Browsing Platform* [online]. [cit. 2019-04-02]. Dostupné z: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

[8] KREMLING, Janine a Amanda M. Sharp PARKER. *Cyberspace, cybersecurity, and cybercrime*. Los Angeles: SAGE Publications, [2018]. ISBN 978-150-6347-257.

[9] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-808-8168-157.

[10] World Internet Users and 2018 Population Stats. *Internet World Stats* [online]. [cit. 2018-12-03]. Dostupné z: https://www.internetworldstats.com/stats.htm

[11] How to Acces the Deep Web. *Deep Web Sites Links* [online]. [cit. 2018-12-03]. Dostupné z: https://www.deepwebsiteslinks.com/how-to-access-the-deep-web/

[12] ROTSCHILD, Mike. 26 Crazy Things You Can Buy on the Dark Web. *Ranker* [online]. [cit. 2018-12-03]. Dostupné z: https://www.ranker.com/list/things-you-can-buy-on-the-dark-web/mike-rothschild

[13] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013. ISBN 978–80–7251–397–0.

[14] ČESKO. § 7 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2018 [cit. 15. 12. 2018]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181#p7

[15] *Council of Europe: Convention on Cybercrime* [online]. In: . Budapest, 2001, European Treaty Series - No. 185. Dostupné také z: https://www.coe.int/en/web/cybercrime/the-budapest-convention

[16] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

[17] HLAVENKA, Jiří. *Výkladový slovník výpočetní techniky a komunikací: 5500 pojmů z oblasti výpočetní techniky : přes 7000 křížových vazeb : výklad anglických a českých odborných pojmů*. 3. vyd. Praha: Computer Press, 1997. ISBN 80-722-6023-5.

[18] POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-868-9838-5.

[19] KOZIEROK, Charles M. *The TCP/IP guide: a comprehensive, illustrated Internet protocols reference*. San Francisco: No Starch Press, c2005. ISBN 978-1593270476.

[20] HADNAGY, Christopher. *Social engineering: the art of human hacking*. Indianapolis, IN: Wiley, c2011. ISBN 04-706-3953-9.

[21] ABU RAJAB, Moheeb, Jay ZARFOSS, Fabian MONROSE a Andreas TERZIS. A multifaceted approach to understanding the botnet phenomenon. *Proceedings of the 6th ACM SIGCOMM on Internet measurement - IMC '06*. New York, New York, USA: ACM Press, 2006, 2006, , 41-. DOI: 10.1145/1177080.1177086. ISBN 1595935614. Dostupné také z: http://portal.acm.org/citation.cfm?doid=1177080.1177086

[22] How a Botnet works. In: *EMSIsoft blog* [online]. 23.5.2017 [cit. 2019-01-24]. Dostupné z: https://blog.emsisoft.com/en/27233/what-is-a-botnet/

[23] Global spam volume as percentage of total e-mail traffic from January 2014 to September 2018, by month. *Statista* [online]. listopad 2018 [cit. 2019-01-24]. Dostupné z: https://www.statista.com/statistics/420391/spam-email-traffic-share/

[24] Number of sent and received e-mails per day worldwide from 2017 to 2022 (in billions). *Statista* [online]. listopad 2018 [cit. 2019-01-24]. Dostupné z: https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/

[25] JAGATIC, Tom, Nathaniel JOHNSON, Markus JAKOBSSON a Filipo MENCZNER. *Social phishing*. Bloomington, 2005. Class project. Indiana University.

[26] ERICKSON, Jon. *Hacking: the art of exploitation*. 2nd ed. San Francisco, CA: No Starch Press, c2008. ISBN 978-1-59327-144-2.

[27] MATĚJKA, Michal. *Počítačová kriminalita*. Praha: Computer Press, 2002. ISBN 80-722-6419-2.

[28] HAFNER, Robert, Harry van TIL, Sofie ROHLFS, Martin van der ENDE, Patrick de BAS, Anastasia YAGAFAROVA a Joost POOR. *Estimating displacement rates of copyrighted content in the EU*. Brusel, 2015. ISBN 978-92-79-35136-5.

[29] NEWMAN, Lily Hay. GitHub Survived the Biggest DDoS Attack Ever Recorded. *Wired* [online]. 1. 3. 2018 [cit. 2019-01-30]. Dostupné z: https://www.wired.com/story/github-ddos-memcached/

[30] DDoS Attacks 2018: New Records and Trends. *Calyptix Security* [online]. 10. 8. 2018 [cit. 2019-01-30]. Dostupné z: https://www.calyptix.com/top-threats/ddos-attacks-2018-new-records-and-trends/

[31] MARAS, Marie-Helen. *Cybercriminology*. New York: Oxford University Press, [2017]. ISBN 978-0-19-027844-1.

[32] SVOBODOVÁ, Ivana. To dítě utopit!. *Respekt* [online]. 17.2.2018, **2018**(8) [cit. 2019-01-30]. ISSN 1801-1446. Dostupné z: https://www.respekt.cz/tydenik/2018/8/tema-to-dite-utopit

[33] SVOBODOVÁ, Ivana. Soudy potrestaly dva lidi, kteří na Facebooku přáli smrt dítěti. *Respekt* [online]. 9.1.2019 [cit. 2019-01-30]. Dostupné z: https://www.respekt.cz/respekt-pravo/soudy-potrestaly-dva-lidi-kteri-na-facebooku-prali-smrt-diteti

[34] HOLLÁ, Katarína. *Sexting a kyberšikana*. Bratislava: IRIS, 2016. ISBN 978-80-8153-061-6.

[35] WORTLEY, Richard a Stephen SMALLBONE. *Child Pornography on the Internet*. 2. vydání. Center for Problem-Oriented Policing, 2012. ISBN 1-932582-65-7.

[36] *Cyber crime and cyber terrorism investigator's handbook*. Boston: Elsevier, [2014], s. 13-16. ISBN 978-0-12-800743-3.

[37] *Výroční zpráva NCOZ 2018* [online]. In: . [cit. 2019-03-02]. Dostupné z: https://ct24.ceskatelevize.cz/sites/default/files/2217752-vyrocni_zprava_ncoz.pdf

[38] European Cybercrime Centre - EC3: Combating crime in a digital age. *Europol* [online]. [cit. 2019-03-02]. Dostupné z: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

[39] Cybercrime. *Interpol* [online]. [cit. 2019-03-02]. Dostupné z: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

[40] VOKUŠ, Jiří. Kybernetická kriminalita. In: *Policie ČR* [online]. 14.2.2019 [cit. 2019-03-03]. Dostupné z: https://www.policie.cz/clanek/kyberneticka-kriminalita.aspx

[41] Obyvatelstvo. *Český Statistický Úřad* [online]. 26.3.2019 [cit. 2019-03-27]. Dostupné z: https://www.czso.cz/csu/czso/obyvatelstvo_lide

[42] Každá sranda něco stojí. *Policie ČR* [online]. [cit. 2019-04-06]. Dostupné z: https://www.policie.cz/clanek/kazda-sranda-neco-stoji.aspx

[43] PIERCE, Robert Lee. *Child pornography: A hidden dimension of child abuse*. 1984, **8**(4), 483-493. DOI: 10.1016/0145-2134(84)90030-9. ISSN 01452134. Dostupné také z: http://linkinghub.elsevier.com/retrieve/pii/0145213484900309

[44] ČIHÁK, František. Psychické reakce dětských obětí sexuálního zneužívání a znásilnění. *Pediatrie pro praxi*. Solen, 2011, **2011**(12), 325-327. ISSN 1803-5264.

[45] DAVIS, Keith E., Ann L. COKER a Maureen SANDERSON. Physical and Mental Health Effects of Being Stalked for Men and Women. *Violence and Victims*. 2002, **17**(4), 429-443. DOI: 10.1891/vivi.17.4.429.33682. ISSN 0886-6708. Dostupné také z: http://connect.springerpub.com/lookup/doi/10.1891/vivi.17.4.429.33682

[46] CLARK, Rodney, Norman B. ANDERSON, Vernessa R. CLARK a David R. WILLIAMS. Racism as a stressor for African Americans: A biopsychosocial model. *American Psychologist*. 1999, **54**(10), 805-816. DOI: 10.1037/0003-066X.54.10.805. ISSN

1935-990X. Dostupné také z: http://doi.apa.org/getdoi.cfm?doi=10.1037/0003-066X.54.10.805

[47] JONES, Connor a Siobhan CONNERS. What is Article 13 and Article 11?. *ITPRO* [online]. 1.4.2019 [cit. 2019-04-06]. Dostupné z: https://www.itpro.co.uk/policy-legislation/32552/what-is-article-13-and-article-11

[48] Fámy o únosech dětí spustily ve Francii vlnu útoků na Romy. Násilí se stupňuje i v Itálii. *ČT24* [online]. 6.4.2019 [cit. 2019-04-06]. Dostupné z: https://ct24.ceskatelevize.cz/svet/2780060-famy-o-unosech-deti-spustily-ve-francii-vlnu-utoku-na-romy-nasili-se-stupnuje-i-v

[49] LEWIS, James. Economic Impact of Cybercrime—No Slowing Down. *McAfee* [online]. únor 2018 [cit. 2019-04-07]. Dostupné z: https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email

[50] Registered cases of cybercrime in Belgium from 2007 to 2017. *Statista* [online]. [cit. 2019-04-07]. Dostupné z: https://www.statista.com/statistics/534977/cybercrime-in-belgium/

[51] SHALAL, Andrea. Germany sees rise in cybercrime, but reporting rates still low. *Reuters* [online]. 5.3.2017 [cit. 2019-04-07]. Dostupné z: https://www.reuters.com/article/us-germany-cybercrime-crime/germany-sees-rise-in-cybercrime-but-reporting-rates-still-low-idUSKBN17Z26S

[52] EUR průměrné kurzy 2016, historie kurzů měn. *KurzyCZ* [online]. [cit. 2019-04-07]. Dostupné z: https://www.kurzy.cz/kurzy-men/historie/EUR-euro/2016/

# 9 SEZNAM POUŽITÝCH OBRÁZKŮ

# 10 SEZNAM POUŽITÝCH TABULEK

# 11 SEZNAM POUŽITÝCH GRAFŮ